Anno 3 – N. 45
26 Febbraio 2004 - 11 Marzo 2004

Direttore Responsabile: Luca Sprea

I Ragazzi della redazione europea:
grand@hackerjournal.it, Bismark.it, Il Coccia, Gualtiero Tronconi, Ana Esteban, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

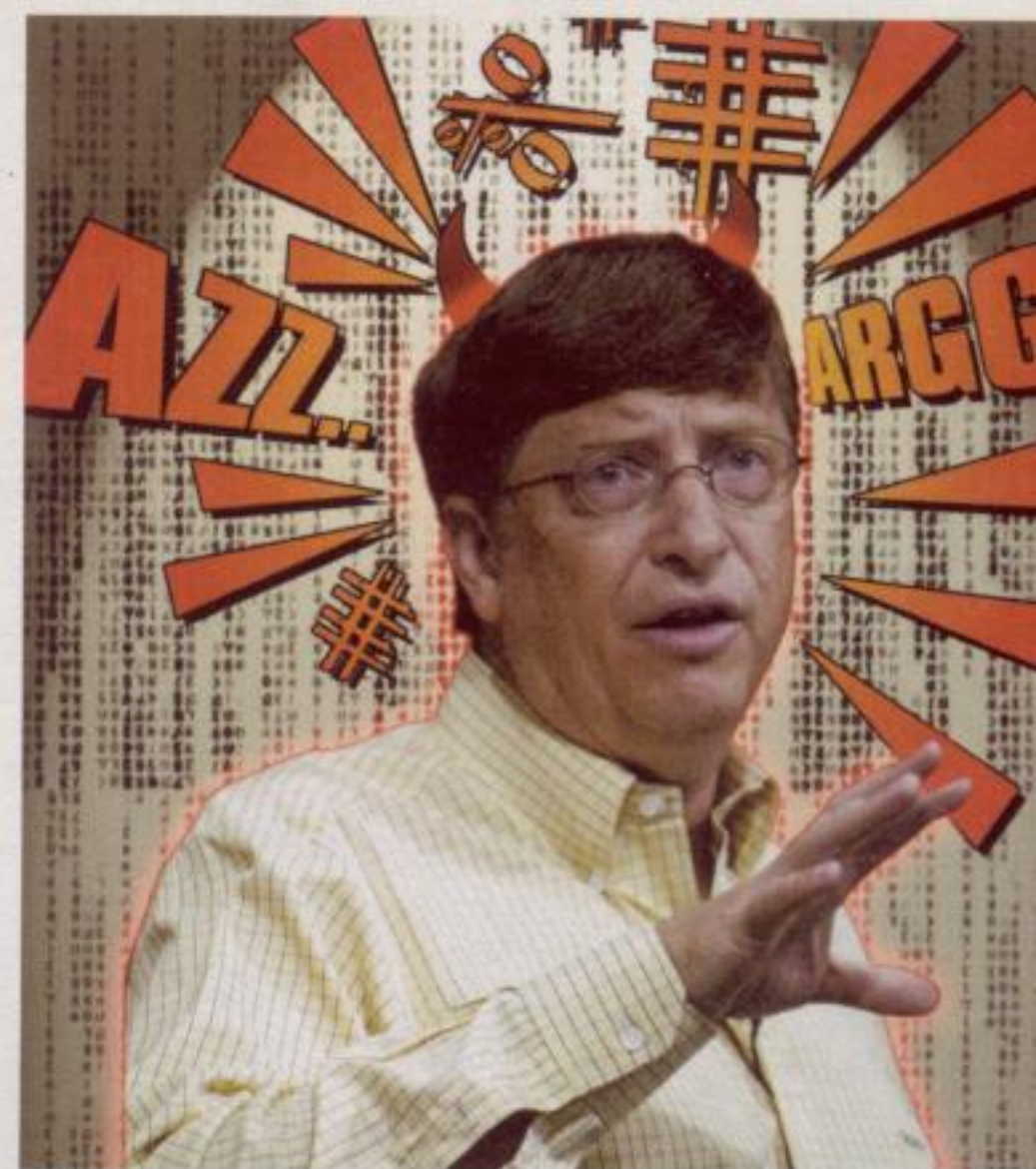
Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Pubblicazione quattordicinale registrata al Tribunale di Milano
il 27/10/03 con il numero 601.

Rubata parte del codice sorgente di Windows 2000 ed NT. Ci aspetta una nuova ondata di attacchi zero-day?

Il FURTO del SECOLO

12 febbraio 2004: Microsoft ha confermato attraverso un comunicato stampa (http://www.microsoft.com /presspass/press /2004/Feb04/02-12windowssource.asp) che alcune porzioni di codice sorgente di Windows 2000 e NT 4.0 sono state trafugate e pubblicate su Internet.

Il codice sorgente recuperabile su Internet è pari a circa 300 MByte zippati, una piccola percentuale rispetto al totale di Windows. Ma ciò che preoccupa è certamente come sia potuto accadere. Le notizie più aggiornate indicano il responsabile in Mainsoft (http://mainsoft.com/), azienda da molto tempo partner tecnologico di Microsoft, uno di quelli che accesso al codice sorgente in questione. Su Internet sono arrivati in totale 30.915 file, per circa 13,5 milioni di righe di programma, provenienti da un computer Linux usato da Mainsoft a scopo di sviluppo e riguardanti il Service Pack 1 di Windows 2000. Probabilmente il computer veniva usato da Eyal Alaluf, Director of Technology di Mainsoft, e il codice era lì per aiutare Mainsoft nello sviluppo del suo prodotto MainWin. Fino al 2001, quando Microsoft ha varato la sua Shared Source Initiative, Mainsoft era una delle due sole aziende autorizzate a vedere i sorgenti di Windows.

Di tutta la vicenda non preoccupa l'aspetto piratesco: dal codice in giro non si può arrivare a software funzionante. Aumenta invece la possibilità di attacchi del genere zero-day.
Un attacco zero-day si basa su una vulnerabilità software che diventa nota all'aggressore prima che lo sappia lo stesso produttore del software. Il malintenzionato ha modo di scrivere codice che sfrutti la vulnerabilità prima che l'azienda riesca a chiudere il buco e disporre di ore, giorni o settimane in cui tutta la base di utenza è a rischio, in attesa che arrivi una patch. Se la parte di codice rubata consente di scrivere codice ostile, il rischio di un attacco zero-day è paurosamente alto. basta pensare a tutte le vulnerabilità che già ci sono nel momento in cui il codice sorgente non è in Rete!

CODICE RUBATO

La vicenda dei codici sorgente rubati a Microsoft non finisce di convincere. È davvero possibile che parti di codice di Windows NT e 2000 possano essere state trafugate così facilmente? Come mai solo una parte del codice è stata rubata? I dubbi sono molti e molte le domande che gli osservatori più attenti si stanno ponendo in queste ore. Chi sarebbe davvero avvantaggiato dalla divulgazione di questi codici? È chiaro che sono di fatto comunque inutilizzabili, sono di proprietà di Microsoft e nessun programmatore, specialmente dell'area open source, sarebbe così sciocco da inserirli in un programma. Davvero c'è un pericolo sicurezza? O si tratta di allarmismo ingiustificato, o ancora di abili mosse di marketing della stessa Microsoft che si è inventata anche questa mossa per cercare di far migrare i propri utenti alle versioni più aggiornate? Molte ipotesi sono verosimili, ma lasciano anche piuttosto perplessi e, soprattutto, non hanno prove a confutarne la veridicità. Ecco alcune "voci di corridoio" che abbiamo raccolto sui principali forum e siti italiani.

I commenti ufficiali Microsoft Italia

Indagini in corso per la pubblicazione illegale sul Web del codice di Windows, nessun rischio per i clienti.

"Giovedì sono state illegalmente rese disponibili su Internet alcune porzioni di codice sorgente apparentemente parte di Microsoft Windows NT 4 e Microsoft Windows 2000. Sono in corso accertamenti per comprendere se si tratti realmente di parti del codice sorgente di prodotti Microsoft e quali aree dei prodotti possano essere coinvolte. Il codice reso disponibile rappresenterebbe solo una piccola porzione del codice sorgente di Microsoft Windows NT 4 e Microsoft Windows 2000.

La pubblicazione illegale di questo codice ha implicazioni a livello legale e di protezione della proprietà intellettuale e non rappresenta un problema di sicurezza per i clienti dei prodotti Microsoft eventualmente coinvolti.

Stiamo collaborando con le autorità per identificare eventuali responsabilità e per intraprendere le azioni più appropriate", ha dichiarato Davide Viganò, Vice Direttore Generale Business Marketing Organization di Microsoft Italia.

Perché a Microsoft conviene?

❶ **i codici trafugati gettano ombre sulla sicurezza dei sistemi esistenti,** fornendo un'ottima carta a chi dovrà "piazzare" i prossimi.

❷ **se le leggi antitrust sui sorgenti possono motivare una sentenza contro Microsoft, non c'è motivo di applicarle quando si tratta di sorgenti ormai trafugati.** In pratica l'immagine di Microsoft si trasforma, davanti all'opinione pubblica e davanti ad eventuali giurie, da quella di un colosso monopolista aggressivo a quella di una vittima, e se l'oggetto del contendere erano codici sorgenti, ecco che tutto il castello accusatorio crolla: i sorgenti sono già nelle mani di tutti, come accusare Microsoft di detenerne il monopolio?

❸ **Gli affari di MS in Europa sono fortemente penalizzati proprio dalla posizione di Microsoft davanti all'Antitrust europea;** nel caso questa posizione si ammorbidisse, i potenziali clienti sarebbero automaticamente portati ad acquistare prodotti con codice sorgente non "pubblico", ciò che MS vuole di più.

Quanto vale il codice "trafugato"? Forse meno dei tre miliardi di dollari di multa che l'Antitrust europea avrebbe potuto chiedere a Microsoft proprio per il monopolio del codice in oggetto, costringendola poi a fare ciò che è accaduto: a metterlo a disposizione dei concorrenti.

❹ **Nessun hacker lascerebbe mai un indirizzo email in mezzo alle righe di codice che trafuga, tanto più quello di un partner MS.** In un caso significherebbe farsi identificare, nell'altro far identificare una fonte che, finchè rimanesse segreta, sarebbe potenzialmente utile anche per altre "operazioni".

Ora:

- il codice è disponibile per i concorrenti e anche per tutti gli altri, concorrenti dei concorrenti inclusi.
- Non è pensabile che MS venga multata per il monopolio di qualcosa che non ha più.
- i procedimenti Antitrust sono da rifare in base agli accertamenti sulla quantità e sulla qualità del codice diffuso.

MI FA RIDERE L'ASSURDITÀ DI QUESTA STORIA

È un caso mondiale che giri il codice di MS. Qual è la differenza tra scaricare un mp3, un programma da p2p e il codice sorgente di microsoft? Nessuna. Per tutte queste cose si viola il copyright. Adesso vogliono farci credere che scaricare i sorgenti di win2k è molto più grave che scaricare un mp3.

Ma mi faccia il piacere! L'opportunità ghiotta è, invece, di dare un occhiata dentro questi codici per vedere se sono stati scritti male o scopiazzando l'open source. Adesso MS ha paura che qualcuno gli copi il proprio codice, ma chissà quante volte "ha preso spunto" dagli altri.

Del resto le finestre l'ha inventate prima la apple... il protocollo tcp-ip all'inizio non era supportato da windows (chi si ricorda il trumpet?), ma era nativo di unix...

(fonte: punto-informatico.it)

Per dire a tutti "beh, dovete passare a XP, visto che quei cattivi bambini ci hanno rubato il codice di w2k"?

Non vi ricordate come ci siamo caduti tutti al finto incrocchiamento di win95 (schermata blu che entra di lato creata ad arte?) Non notate come nessuno passa a XP/2003 server?

Non avete capito la genialità (nel bene e nel male) del buon B.Gates?

A me torna tutto: ci facciamo fottere un po' di codice (magari alla fine si scopre che non serve a niente), poi dichiariamo che w2k, a causa del furto, non è più il caso di usarlo, e consigliamo a tutti di passare a w2003 (che nessuno praticamente sta comprando....)

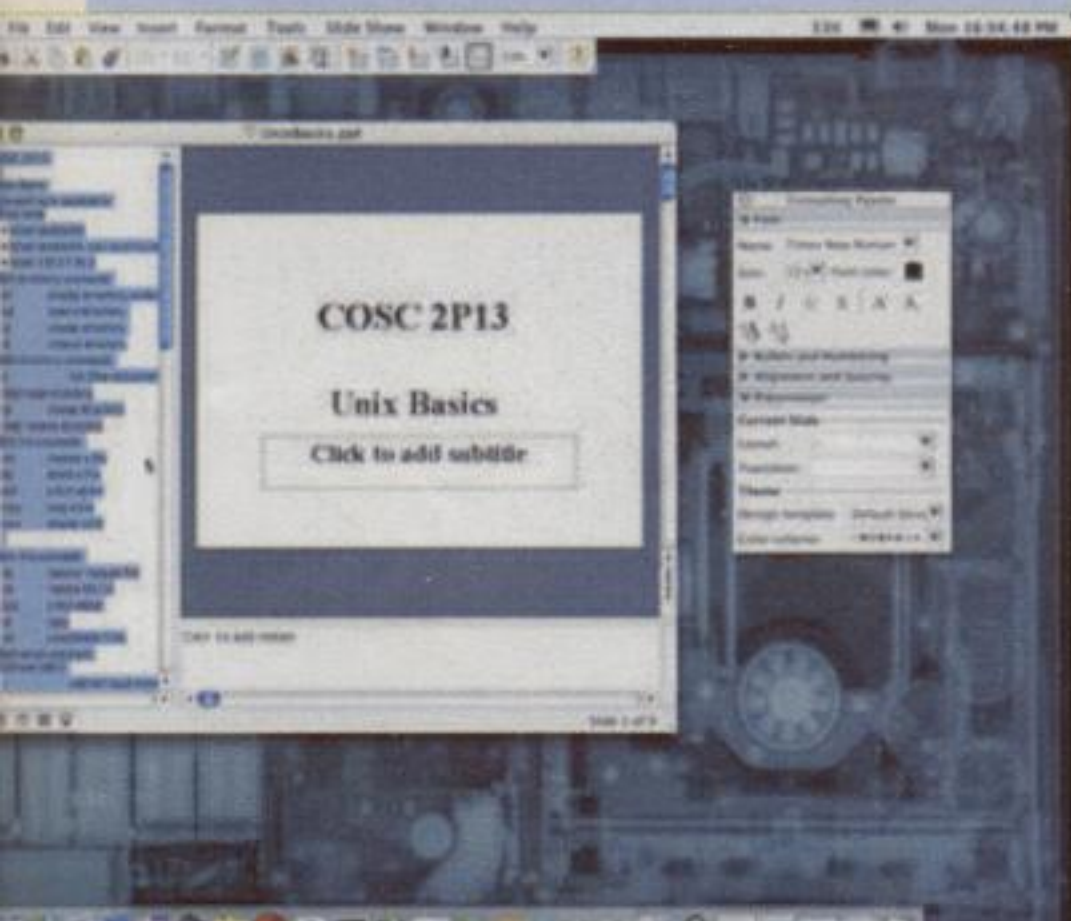
Che ne dite, fantainformatica?

(fonte: punto-informatico.it)

POWERPOINT DA WIN A MAC

Devo aprire con Xp una presentazione in PowerPoint realizzata con un Mac, per comprimere e riformattare il testo. Potreste voi suggerirmi un tool adatto a permettermi questa operazione?

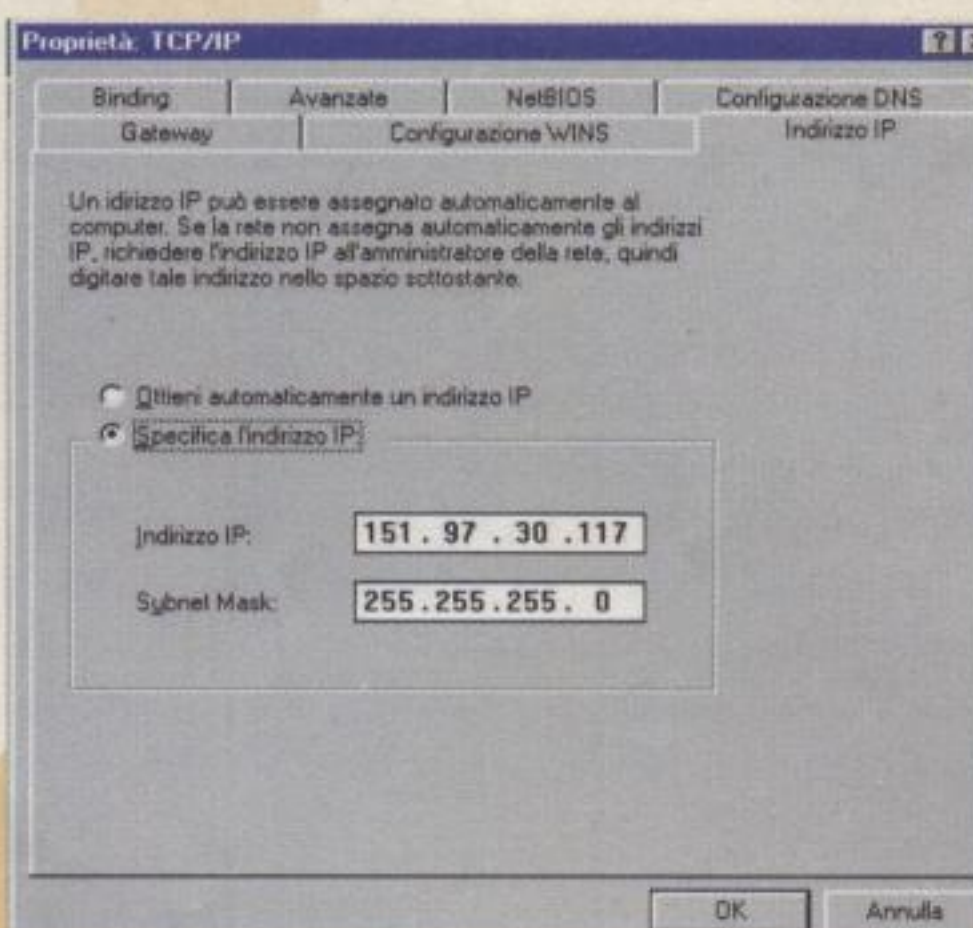
Ubjmaior

Ciao Ubjmaior!
Una delle due: o ti basta applicare al nome file il suffisso .ppt (o .pps) e lo apri tranquillamente con il tuo PowerPoint, oppure chiedi all'autore del file Mac di registrare nuovamente il file, in formato PowerPoint per Windows, dove lo aprirai altrettanto tranquillamente.

▲ *I file PowerPoint funzionano su Windows così come su Mac, ma su Windows devono avere obbligatoriamente l'estensione nel nome file*

IMPARA L'IP E METTILO DA PARTE

Grandissima redazione, vorrei sapere come faccio a conoscere l'indirizzo IP del mio computer. Grazie.

Matteo

Dipende da che computer hai, ma in generale devi andare nei pannelli di controllo e cercare le sezioni riguardanti Internet e, in particolare, TCP/IP. Se sei collegato a Internet mediante un provider che ti fornisce un indirizzo IP dinamico, quest'ultimo sarà sempre diverso a ogni connessione.

▲ *Pannello di Controllo -> Rete -> Proprietà - > Indirizzo IP. Eccolo qui!*

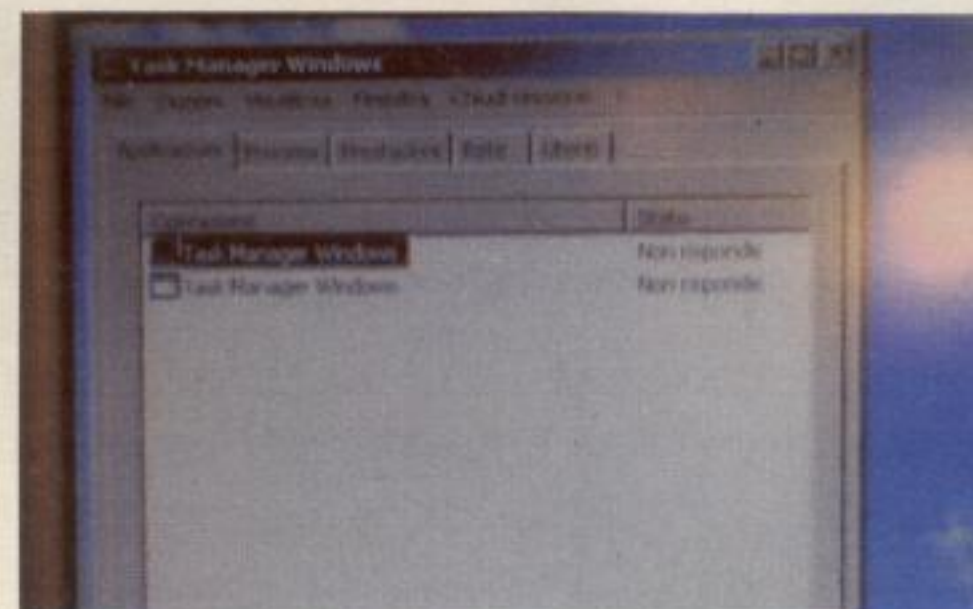
INFO SU SOLARIS

Buongiorno,
mi interesserebbe sapere dove posso trovare una guida abbastanza completa per Solaris 5.6 e per le SPARCstation Sun 10.

Ema

Dovresti cominciare da http://wwws.sun.com/software/solaris e in generale dal sito di Sun, http://www.sun.com, dove troverai un sacco di documentazione. Più avanti cerca un buon libro in argomento su Amazon (http://www.amazon.com) o Internet Bookshop (http://www.internetbookshop.it).

ANCHE TASK MANAGER SI IMPALLA

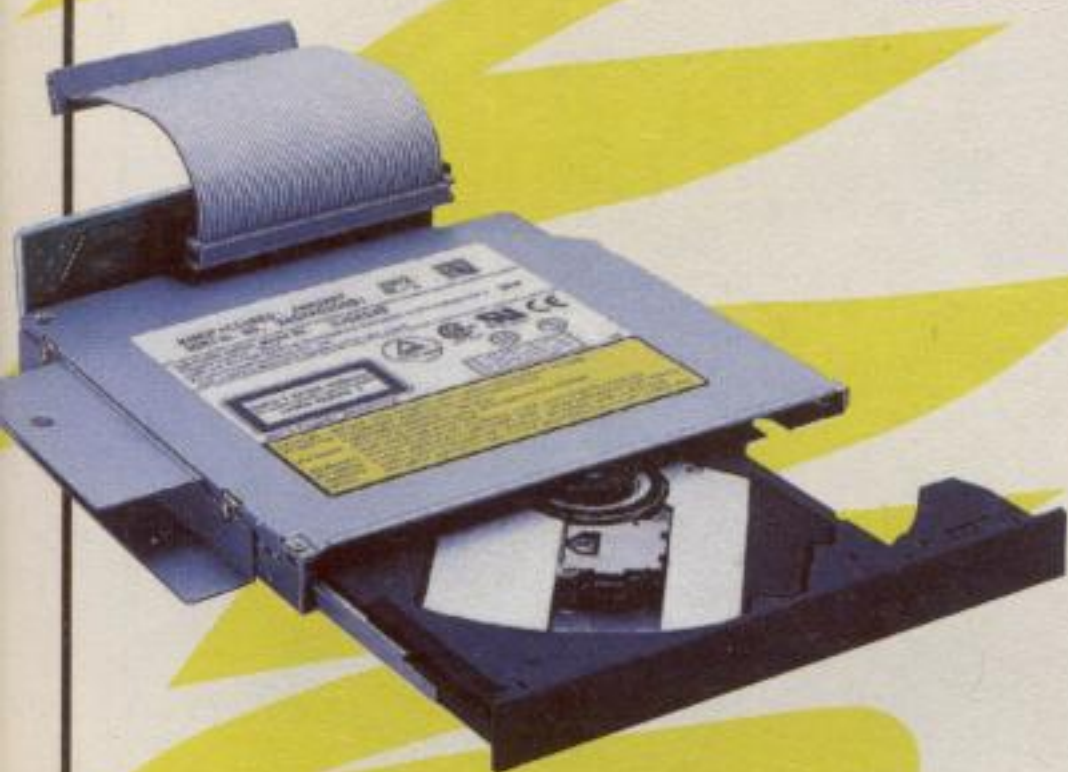
Carissima redazione,
tempo fa ho visto una vignetta con una foto del task manager di windows xp impallato.
La cosa mi fece sorridere non poco!
Bene, proprio l'altra sera a me è successa questa cosa, che a dir la verità non credevo possibile o quanto meno improbabile!
A un certo punto ho dovuto terminare explorer dal task manager, per cercare di far ripartire il tutto senza dover riavviare...

Beh! sorpresa delle sorprese quando ho cercato di far ripartire Explorer dal task manager, si è impallato tutto, e provando la consueta combinazione di tre tasti (forse la cosa più geniale di windows :-) il task manager era IMPALLATO!
Ora non sono un'utente esperto, e non so dirvi se è una cosa usuale, ma non credo...
In allegato trovate la foto dello schermo del mio PC scattata con il cellulare; non è nitidissima, ma era l'unico modo per documentare il fatto visto che non ho una macchina digitale e tanto meno potevo catturare l'immagine dello schermo!

Lancillotto

Grazie, Lancillotto!
No, non è uno spettacolo usuale. La foto mostra quello che deve mostrare e quindi va benissimo. A presto!

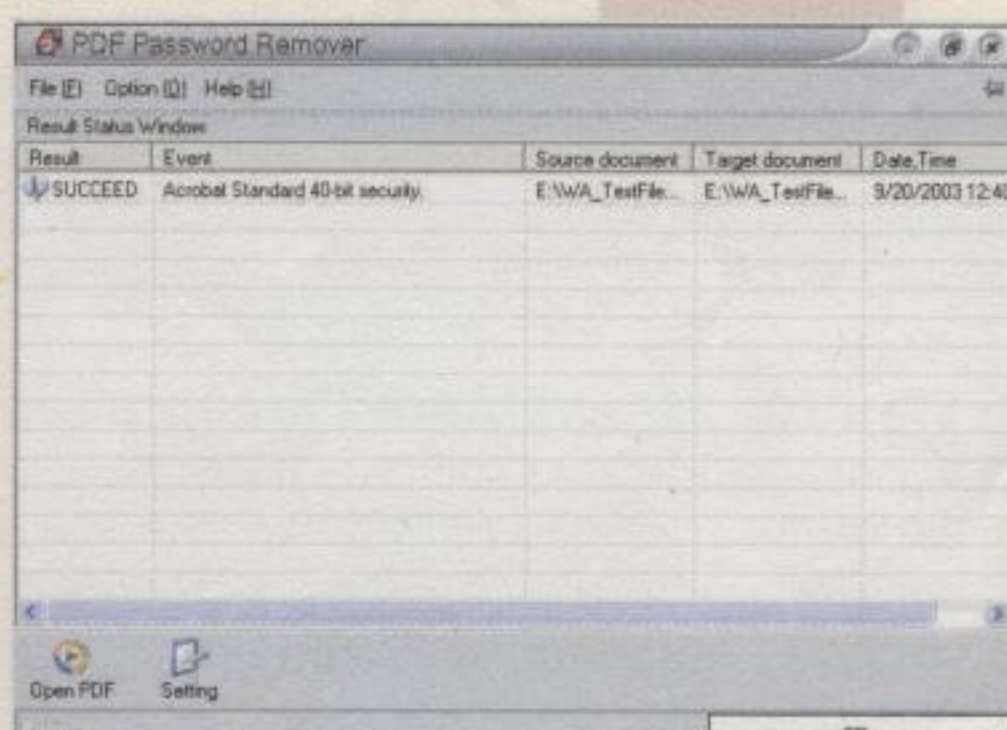
ANDARONO PER MASTERIZZARE...

Ragazzi pongo un mio problemino diciamo così ke m affligge da tempo, da quando ho preso il masterizzatore ke sogno di CREARE una protezione efficace sui miei cd personali in modo da non farli copiare da altri masterizzatori, sapete aiutarmi? spero ke esista qualcosa del genere.

M@rk0

Caro M@rk0,
non puoi pretendere di essere l'unico ad approfittare della riproducibilità del digitale! Scherzi a parte, hai pensato di cifrare il contenuto dei CD? Rimangono copiabili, ma la password per leggerli ce l'avresti solo tu.

BYPASSARE LA PASSWORD DEI PDF

Salve gentile redazione,
ad essere sincero sono un lettore molto recente della vostra rivista. Ho 29 anni ma non ho mai avuto la passione del programmatore; mi sono sempre limitato ad usare i programmi che il mercato mette a disposizione. Ho installato Acrobat 6.0 Professional che mi consente tra le altre cose di poter scrivere su documenti in PDF.
Ho inserito una password su alcuni documenti per evitare di farli scrivere da chi li riceveva... ho smarrito la PW! La domanda è: esiste un modo per (diciamo così) craccarla? O meglio ancora, quando il programma mi chiede di inserire la pw, c'è un programmino che si preoccupi di generarla? Ci tengo a premettere che non ne devo fare un cattivo uso. È solo per evitare di dover ricopiare tutto il documento.

Maurizio

Ce ne sono diversi, di programmini. Prova a usare GuaPDF, a http://www.password-crackers.com/crack/guapdf.html.

QUALCHE DUBBIO SU NETSEND

Ciao Reed,
Vorrei capire come fare a mandare messaggi anonimi tramite NetSend.... ho cercato tramite Google, ma il massimo che ho trovato è stato un programmino di nome "Anetsend", ho provato ad effettuare il reverse engineering con risultati tutt'altro che soddisfacenti. La mia era curiosità sul servizio Net, pertanto del programma non me ne faccio molto, perchè vorrei capire il funzionamento direttamente dalla shell. Il mio interesse per il servizio Net Send era partito per gioco, per mandare messaggi anonimi ad alcuni amici...ho cercato di approfondire e dare risposte alla mia curiosità, trovando però poca documentazione al riguardo. Spero in una vostra risposta!

Bladefun

Ciao Bladefun!
Il funzionamento di Net Send dalla shell è semplice: dai il comando net send nomeutentesullarete testomessaggio. La parte critica è la terza, il nome utente sulla rete. Devi conoscerlo o non potrai inviare messaggi a quell'utente. Per chiarezza, non puoi mandare messaggi anonimi tramite net send. Meglio, non molto anonimi. Il destinatario vede il nome utente del mittente, tant'è che in molte aziende viene usato come sistema rudimentale di messaggistica. Puoi fare trucchi e trucchetti, ma basta un amministratore di rete un po' più solerte del normale a beccarti subito. Se vuoi mandare davvero messaggi anonimi ti consiglio fortemente la posta elettronica.

LE VIE DI GOOGLE SONO INFINITE!

Cari HJ, cercando su google la stringa +"flash plugin" + linux mi è capitato inaspettatamente di trovare, prima delle pagine della Macromedia, questo sito: http://www.geocities.com/TimesSquare/Labyrinth/5084/flash.html che mostra due pgr carini riguardanti flash per linux:)
Dando un'occhiata al sorgente non si trova nulla di starno, anzi, nulla di nulla...
Come avrà fatto il nostro amico a scalare la vetta di Google?

Avrà letto il nostro articolo "Fatti trovare" apparso sul numero 43. :-)

HOT!

CHIP IBM PER GIOCARE SEMPRE MEGLIO

Unendo tutte le supertecnologie che ha impiegato fino adesso per costruire i microprocessori, Ibm è riuscita a iniziare la produzione dell'ultimo chip PowerPC 970, per intenderci il motore degli Xserver G5 di Apple, in una versione che ha chiamato FX e che consuma un sacco di energia in meno. Se ne parlava fin dal 2001, ma solo ora la società, chiamata Big Blue, ha iniziato la produzione di massa. "Così", dicono quelli di Apple, "potremo costruire dei portatili adatti agli sfegatati dei giochi".

MYDOOM È MORTO, VIVA MYDOOM

Il giorno 2 febbraio si è spento il virus MyDoom, o meglio ha automaticamente disattivato la sua potenziale carica distruttrice del sito www.sco.com: era programmato per attaccare quello e c'è riuscito benissimo.

Ma dalle sue ceneri ecco sorgere Nachi-B, l'ultimo rampollo della generazione di virus worm, che tenterà fino a giugno 2004 (quando si spegnerà in modo automatico) di fare parecchie cose:

- eliminare i file di MyDoom A e B
- scaricare dal sito Microsoft una serie di patch per Windows
- tentare di collegarsi, ogni venti minuti, a microsoft.com, google.com e intel.com, provando a infettare di se stesso indirizzi IP generati a caso
- sovrascrivere i file con estensione SHTML, SHTM, STM, CGI, PHP, HTML, HTM e ASP con un file HTML contenente la scritta "LET HISTORY TELL FUTURE !" Per stare tranquilli, è disponibile una patch di Windows reperibile qui: http://www.microsoft.com/technet/security/bulletin/MS03-026.asp

WINDOWS SU CELLULARE? QUASI

Epocware (www.epocware.com) ha sviluppato un software per gli smartphone Sony Ericsson P800/P900 che dà al tutto l'apparenza di un pc, con tanto di desktop.

Sul display si possono mettere collegamenti a numeri telefonici e sms, così come alle applicazioni o agli indirizzi URL, ai file, alle cartelle o ai contatti. L'applicativo è disponibile in italiano, inglese, francese, tedesco, spagnolo, portoghese, olandese, norvegese, svedese e russo. Per qualche prova è disponibile anche una versione trial, ma l'originale costa solamente circa 15 dollari.

UN DISPLAY POTRÀ SUGGERIRTI ALL'ESAME

Potrebbe diventare l'incubo degli insegnanti: un display flessibile, sottile come un foglio di plastica che si può infilare ovunque e che verrà sicuramente utilizzato nei futuri telefonini e per realizzare dispositivi di lettura veramente comodi, come degli e-book di nuova generazione. Immaginatevi lo studente che mentre scrive la soluzione d'esame guarda con noncuranza tra le pagine di un quaderno, dove in realtà è infilato un display collegato a Internet...

È il nuovo display flessibile Philips che unisce alle tecnologie dei 'polimeri organici conduttori' l'uso degli e-ink, particolari inchiostri le cui particelle sono spostate da campi elettrici. Per ora in bianco e nero, promette di essere un buon primo passo verso applicazioni tutte da immaginare.

PILE SUPER POTENTI!

Si chiama Oxyride, è identica alle batterie alcaline a cui siamo abituati, costa uguale e dura circa il doppio. È la nuova tecnologia Panasonic per le batterie usa e getta e nel momento dell'annuncio due batterie AA sono riuscite a spostare un'automobile pesante 18,5 chilogrammi per 1,2 chilometri.

Sarà introdotta ad aprile su tutti i mercati mondiali. La composizione? Zinco per l'elettrodo negativo, ossidruro di nickel (NiOOH) e una nuova preparazione di ossido di manganese (MnO_2) per l'elettrodo positivo, mentre l'idrossido di potassio fa da elettrolita. Come dire: quando l'avrete in mano, non apritela per nessun motivo, perché è tossica e caustica.

LA TV DIGITALE CHE TI LASCIA AL VERDE

Ci siamo quasi: il digitale terrestre apre le porte al browser sul TV. Che è come dire: vedo lo spot di un casinò, posso giocarmi lo stipendio on-line, immediatamente, interattivamente, automaticamente. È quanto visibile in uno dei clip di esempio nel sito www.opentv.com, società che ha fornito a Panasonic la tecnologia per inserire, nei nuovi TV digitali, un browser HTML e BML compatibile. Per ora solamente in Giappone, dove il Broadcasting Markup Language è già operativo. Ma con la presenza dell'interprete HTML, sono pronti ad esportare il tutto anche in casa nostra. Alla larga, TV digitale…

ANCORA! UN 'BUCO CRITICO' IN WINDOWS

L'ultima falla è definita 'critica' e riguarda la debolezza di un metodo utilizzato da Windows per la condivisione delle informazioni, chiamato Abstract Syntax Notation, ASN. Il sistema è utilizzato da tutte le versioni di Windows ed è così inserito nel cuore operativo, che un rimedio è stato rilasciato solamente in questi giorni, a sei mesi di distanza dalla scoperta della vulnerabilità. Ormai è riconosciuto ovunque: Windows è un groviera. I buchi di minore o maggiore importanza non si contano più e nei primi quindici giorni di febbraio sono stati addirittura due i 'warning' da parte di Microsoft rispetto a lacune di sicurezza del sistema.

WINDOWS RIESCE A MINARE MACINTOSH

Nemmeno l'ambiente Macintosh (sia 9.x che X) può stare tranquillo di fronte alle voragini che si aprono nel sistema operativo di Microsoft. Tutti i possessori di Virtual PC sono infatti potenzialmente a rischio di intrusione da parte di qualunque attaccante. È di febbraio la patch rilasciata da Microsoft per aggiornare Virtual Pc e definita 'importante', ovvero al terzo gradino di quattro nella scala di allarme. Altrimenti, sono parole della Grande Mamma, "un attacco ai Mac che stanno facendo girare Virtual PC comporterebbe prendere totale possesso della macchina attaccata". La comunità Mac si unisce tutta e ringrazia…

Severity	Update Number/Software Affected
Critical **Important** Moderate Low	**Security Update 835150** • Virtual PC for Mac 6.0 • Virtual PC for Mac 6.01 • Virtual PC for Mac 6.02 • Virtual PC for Mac 6.1 Get more technical details about this update in Security Bulletin MS04-005

HOT!

TV E PORTATILE DAL FUTURO

Asus ha annunciato un nuovo portatile da design davvero innovativo e futuristico. Le prestazioni sono assolutamente simili a quelle degli altri portatili ora in commercio, ma il design e alcune dotazioni meritano una nota. Il W1, questo il nome del nuovo notebook, è dotato di un sistema audio evoluto, ed è addirittura prevista la presenza di

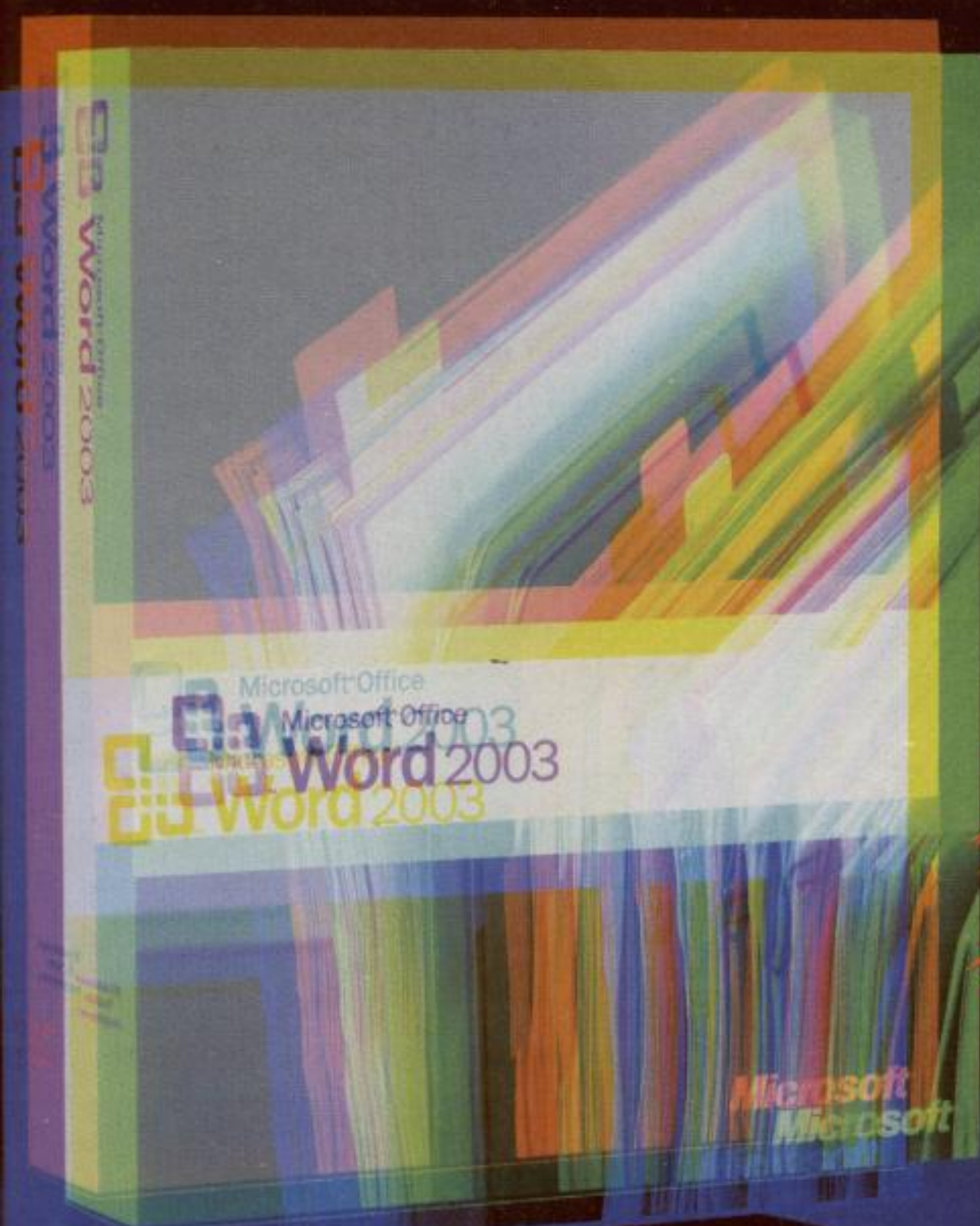
un subwoofer integrato nel fondo. Inoltre è disponibile un piccolo telecomando, che durante il trasporto può essere alloggiato in uno scomparto. La presenza di un sintonizzatore TV integrato, che permette di visualizzare o registare immagini televisive fa capire che questo portatile sostituirà più di un vecchi televisore.

WINDOWS È UNA PAROLA QUALUNQUE

Un corte federale di Seattle ha stabilito che Lindows (http://www.lindows.com), una versione di Linux particolarmente facile da usare e molto curata nell'interfaccia utente, non viola la copyright di marchi registrati e in particolare di Windows, come invece sosteneva Microsoft. In pratica, i giudici hanno stabilito che Windows (finestre, in inglese) è una parola normale, usata quotidianamente da tutti, e che quindi Microsoft non ha diritto di impedire a nessuno di usarla, non importa quanti soldi spenda.

Qualcuno dirà: ci voleva tanto? Gente, Microsoft ha i soldi, e gli avvocati.

VIVA LYX ABBASSO WORD

Altro che Word! I veri geni usano elaboratori di testo come questi, con sotto un motore da paura...

Tanto per dirlo chiaramente: Word è un programma tanto tanto bellino, da guardare, pieno di icone che nessuno usa, gonfio di barre di strumenti inutili, anche bello pesante, nonché portatore di virus, in una parola: Microsoft.

Quando c'è da scrivere testo seriamente, per esempio una tesi, o una ricerca come si deve, ma anche una lettera elegante e ben scritta, niente è meglio di LaTeX, un linguaggio di elaborazione documenti potente ma anche difficile da usare. Ebbene, c'è LyX: un'interfaccia grafica montata sopra LaTeX (http://www.latex-project.org/) che consente di approfittare della potenza di LaTeX senza dover essere scienziati. Le schermate che pubblichiamo in questa pagina parlano da sole.

Il Document Processor

LyX è un elaboratore di documenti, non di testo, perché incoraggia a scrivere pensando alla struttura del documento e non a come il documento apparirà. Perché apparirà giusto! Un esempio, che sconcerta subito chi è abituato a programmi come Word: premere ripetutamente la barra spazio non ha effetto, perché LyX applica automaticamente la giusta spaziatura, in modo intelligente.

In Lyx si lavora definendo alcune regole base e poi concentrandosi davvero sul documento, perché all'impaginazione vera e propria di pensa il programma. Anche se è perfetto per scriverci un curriculum o lettere commerciali, LyX dà il meglio di sé sui documenti lunghi, pieni di note, con sezioni diverse, magari equazioni matematiche. E se si trattasse di migliaia di pagine? Word collasserebbe. LyX non batte ciglio, invece.

▲*I documenti finali prodotti da LyX non hanno niente da invidiare a quelli di un vero editor!*

WYSIWYM

Da quando ci sono le interfacce grafiche si parla tanto di WYSIWYG, What You See Is What You Get, quello che vediamo è quello che stampiamo. Secondo i creatori di LyX è invece cominciata l'era del WYSIWYM: What You See Is What You Mean, cioè quello che vediamo è quello che intendiamo. A significare che LyX crea veramente il documento che vogliamo noi, dove invece in molti casi è il word processor che fa a modo suo quando noi intendiamo un'altra cosa.

Figure, riferimenti a figure, tabelle, equazioni... la potenza di LyX (e del suo motore LaTeX) è senza limiti

Quando andiamo a stampare il risultato di LyX è di qualità assoluta, perché LaTeX, il suo motore, è di livello industriale, tanto che ci sono diverse case editrici che pubblicano libri perfetti basandosi praticamente solo su esso. Per molti LaTeX è un problema, perché il suo uso è molto complicato e un documento scritto in LaTeX somiglia molto al lavoro di un programmatore. LyX è la soluzione, perché consente di usare un motore dalle possibilità infinite senza doversene studiare le macro e le particolarità. Naturalmente una conoscenza di LaTeX aumenta le possibilità a disposizione, proprio come conoscere a menadito l'HTML consente di andare molto oltre quello che consente uno strumento come Dreamweaver. Ma si può iniziare a scrivere buon HTML con DreamWeaver da subito, e intanto mettersi con calma a imparare il linguaggio. Allo stesso modo, LyX dà tutto il tempo di approfondire LaTeX, intanto che i nostri documenti cambiano faccia da subito.

PER SCUOLA, CASA, UFFICIO

Lyx funziona su Windows/Cygwin (il port richiede un server X per funzionare), OS/2, Linux, Mac OS X (nativamente, grazie alla libreria Qt/Mac) e su tutti i dialetti Unix più diffusi. Quindi siamo sicuri di poterlo usare su qualsiasi computer. Inoltre è disponibile il set di comandi in italiano. Non manca davvero niente! Ed essendo open source il software diventa sempre più ricco di giorno in giorno.

Barg the Gnoll
gnoll@hackerjournal.it

DOPPIA

DOPPIA

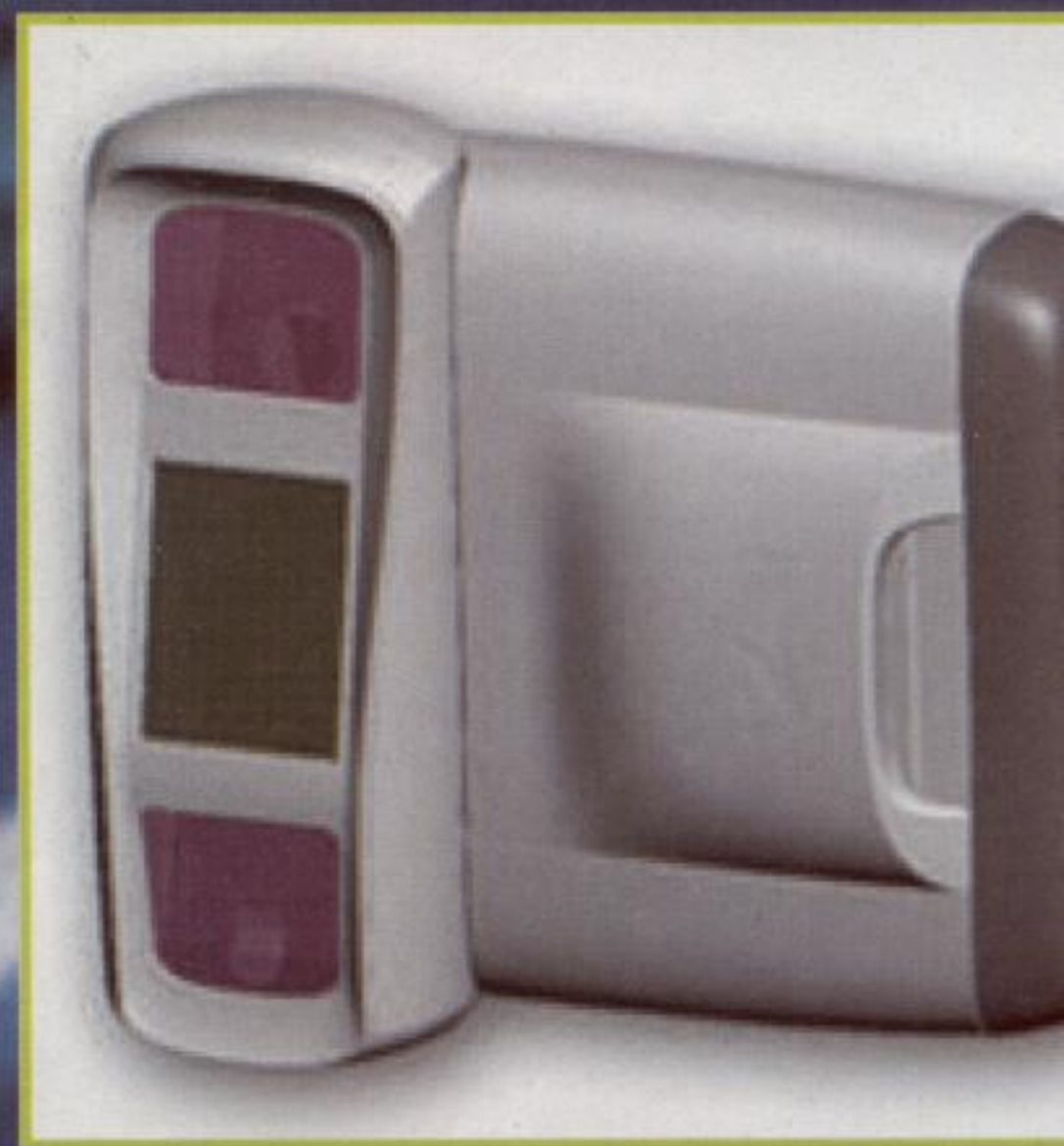
Applichiamo al nostro computer le avanzate tecnologie di riconoscimento facciale in uso negli aeroporti... e inganniamole

È sufficiente il un PC per mettere in piedi uno straordinario sistema di riconoscimento facciale, capace di proteggere il nostro computer da intrusioni di estranei.
L'unica cosa che dovremo fare è sederci davanti a lui e fargli un bel sorriso.

Cosa ci serve

Il software di riconoscimento lavora con qualunque PC Windows collegato a una WebCam. Si chiama VideoLock di Alparysoft e dopo l'installazione ha solamente bisogno di essere addestrato.
Una funzione di training riempie un database di immagini, circa una decina sono sufficienti, con la nostra bella faccia. Meglio se faremo qualche ripresa con angolazioni differenti e con luci differenti e, possibilmente, con espressioni differenti. Su, un bel sorriso!
L'algoritmo utilizzato dal sistema di riconoscimento è ricavato direttamente dagli stessi metodi dei sistemi più sofisticati, ora in uso in tutti gli aeroporti principali, negli stadi e in alcune città soprattutto statunitensi.
Certamente l'installazione su PC è una versione più semplice e più agile di quella che confronta le facce di migliaia di persone con un database di schedati dalle polizie di tutto il mondo, ma il risultato è, più o meno, identico.

2D senza profondità

Questo software fa uso di un algoritmo che nei sistemi di riconoscimento facciale è classificato di prima generazione, perché è puramente bidimensionale. Significa che il riconoscimento avviene perché innanzitutto individua alcuni tratti caratteristici che

Una camera di ripresa 3D, per un riconoscimento più accurato

IDENTITÀ

sono presenti in tutti i volti umani, anche se solamente fotografati. Quindi costruisce una particolare impronta facciale facendo uso di altri punti specifici e differenti, presenti in ciascun volto. Ricava quindi una stringa di bit unica e individuale, che gli consentirà il confronto con le stringhe memorizzate nel database. Negli algoritmi più recenti il software è tridimensionale, per cui il riconoscimento avviene su una ripresa fatta da telecamere con due dispositivi ottici, le cui immagini vengono poi rielaborate e confrontate, ottenendo delle ricostruzioni di impronte facciali molto più accurate e, soprattutto, a prova di... fotografia.

Come ingannarlo

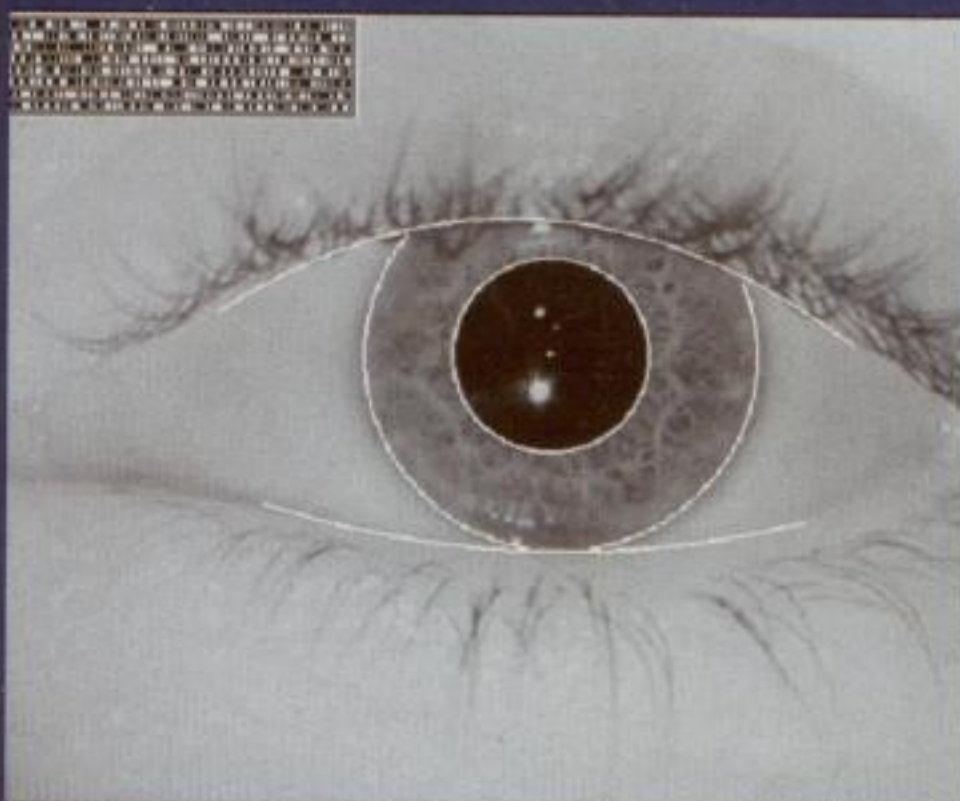
Sì, perché il punto debole del sistema che abbiamo appena impostato sul nostro PC è proprio questo: non è capace di capire se la faccia che ha davanti è reale oppure no.
Questo significa che ci riconoscerebbe anche se mettessimo una fotografia davanti alla WebCam. E finché siamo noi, nessun problema, ma se è qualche nostro scaltro nemico che ci ha ripreso con una semplice macchina fotografica, sono guai.

La prova

Faccio una foto alla mia ragazza (vedi figura 1) e la stampo in bassa risoluzione su una banalissima stampante a getto d'inchiostro. Vado davanti al suo computer e riprendo, con la WebCam, la foto appena stampata. Il software non ha dubbi: non solo è una faccia, ma è anche riconoscibile. Entro nel suo portatile in un batter d'occhio. Sperando che non mi scopra...

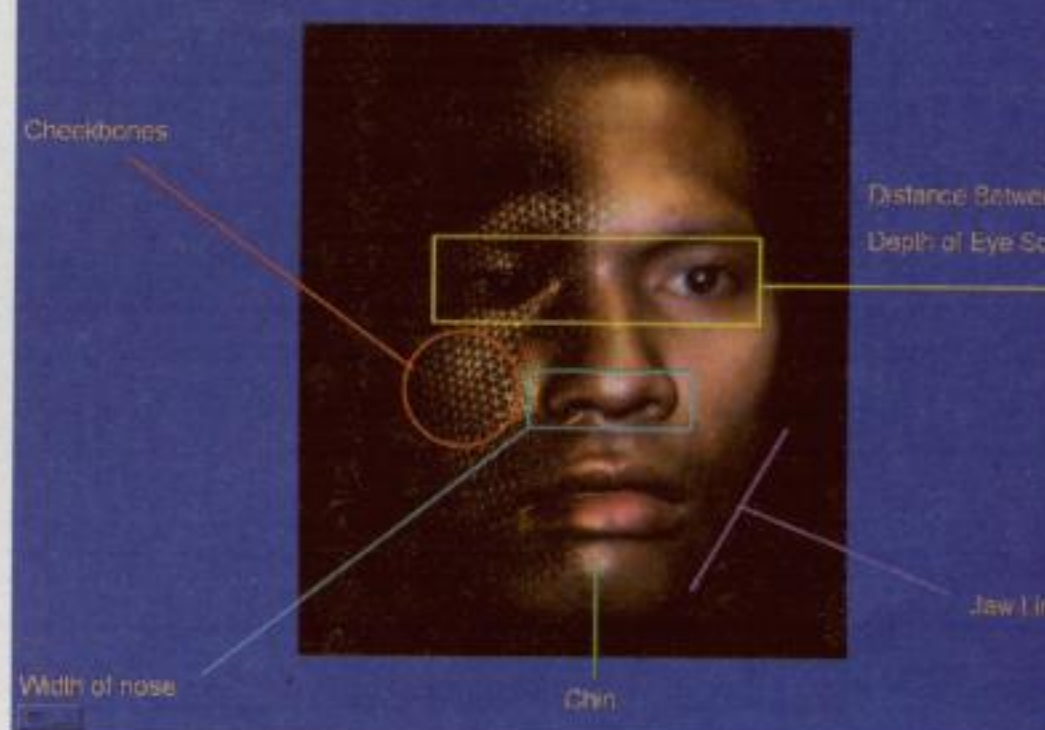
Piazzo la sua immagine stampata davanti alla WebCam del suo computer, che è protetto con il software di riconoscimento facciale

La difesa

Non c'è difesa, possiamo solamente sperare che chi è riuscito ad accedere al computer non sia andato a cancellare il log che lo stesso software mantiene, contenente tutti i riconoscimenti effettuati, sia quelli che sono

andati a buon fine, sia quelli dei tentativi fraudolenti. Perlomeno adesso lo sappiamo e potremo divertirci.

TIPS

COME FUNZIONA

Nel volto umano ci sono tratti caratteristici e comuni a tutti che lo rendono, appunto, 'umano'. Da parecchi anni si studiano queste caratteristiche e i risultati sono sorprendenti. Una delle prime tecniche biometriche applicate anche in Italia, in via sperimentale addirittura ai bancomat, è stata quella del riconoscimento dell'iride. Anche l'iride

è una sorta di impronta digitale che ci rende univoci e diversi da qualunque altra persona la mondo. Tramite il riconoscimento dell'iride è sufficiente presentarsi davanti allo sportello bancario – se è così attrezzato , inserire il tesserino e guardare dritti davanti a sé. Niente più codici da ricordare e password da perdere.
Anche il riconoscimento della faccia è ormai sufficientemente preciso. Forse non ancora al punto da affidargli i nostri risparmi, ma certamente utile alle polizie di mezzo mondo per monitorare in tempo reale il passaggio della gente in aree protette o a rischio. Privacy permettendo.

Le tecniche utilizzate da Al Qaeda per la trasmissione dei messaggi cifrati derivano da quelle usate dagli antichi greci, dagli indiani Navajo, e da quelle usate nella Germania nazista

STORIA dei messaggi

Il segreto del Re

Erodoto di Alicarnasso, il famoso storico greco, racconta nel ventunesimo logos delle sue Storie di un ex Re spartano in esilio, Demarato. L'anno è il 480 aC. e Serse, Re della Persia, volle incontrare Demarato e lo informò dei suoi piani di conquistare l'intera Grecia, invadendola con un gigantesco esercito forte di un milione e settecentomila uomini trasportati su una flotta di ben milleduecentosette navi. Demarato, che pure mancava da oltre un decennio da Sparta evidentemente amava ancora la sua patria e decise così di far arrivare in Grecia un messaggio segreto. Ma come evadere la sorveglianza dei persiani? Demarato prende una tavoletta di creta coperta da cera d'api, sulla cui superficie ai tempi si soleva scrivere, e la ripulisce da tutta la cera. Incide poi il messaggio segreto sulla creta stessa. Infine scioglie nuovamente la cera e la usa per coprire il messaggio in modo che risulti invisibile. La tavoletta viene allora inserita in un trasporto insieme a molti altri supporti davvero vergini e viene trasportata sino in Grecia. Gli Spartani, così preavvertiti, poterono organizzare una forma di resistenza: da qui nacque la famosissima battaglia inscenata da Leonida e dai suoi trecento compagni d'armi alle Termopili (era stata la moglie di Leonida a scoprire il messaggio nascosto sotto la cera). Oggi i terroristi di Al Qaeda utilizzano sostanzialmente lo stesso trucco di Demarato per passarsi messaggi segreti cercando di eludere la sorveglianza dei servizi segreti statunitensi. La tecnologia che permette di nascondere messaggi ha anche un nome: noi la chiamiamo stèganografia. Appropriatamente, il termine viene dal greco: stèganos significa segreto. Per Al Qaeda il compito è più semplice che per Demarato: nell'era di Internet esiste una infinità digitale di informazioni dentro le quali nasconderne altre. Un semplice ma interessante metodo steganografico digitale si chiama "snow" e prevede l'invio di un lungo messaggio di posta elettronica dall'aspetto innocente. Ciascuna riga di testo del messaggio, però, contiene in coda un certo numero di spazi bianchi. Contando e osservando la disposizione di quegli spazi, il vero messaggio segreto emerge agli occhi del destinatario.

Il cifrario dell'imperatore

Nel suo Vite dei Cesari, lo storico romano Svetonio racconta di uno stratagemma inventato da Giulio Cesare. Il grande generale doveva inviare spesso messaggeri con ordini urgenti ai suoi comandanti militari, ma temeva che qualcuno potesse intercettare il cavaliere, impadronirsi della sua sacca dei documenti e scoprire così i piani dell'esercito romano. Cesare si era dunque messo d'accordo con i suoi ufficiali e vergava gli ordini usando un codice. Ogni lettera del messaggio veniva sostituita con la lettera che la segue di tre posti nell'alfabeto. Quindi ogni A veniva rimpiazzata da una D, ogni B con una E, ogni C con una F e così via fino alla Z che veniva scambiata con una C. Di conseguenza i nemici che, per fortuna o per abilità, riuscivano a posare gli occhi sui dispacci di Giulio Cesare non riuscivano a comprenderli. Varianti un po'

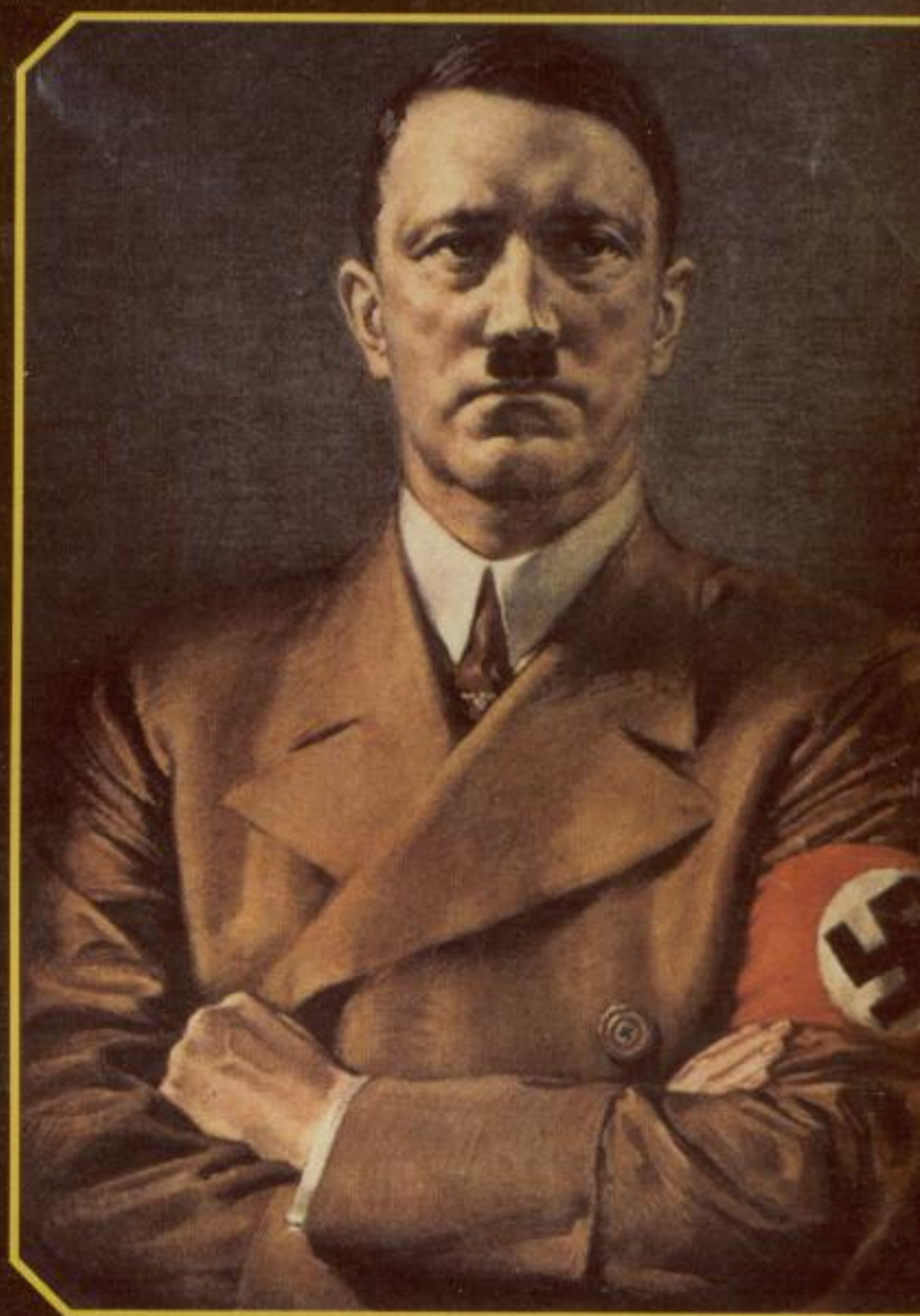
SEGRETI

più complesse del codice cesareo vennero utilizzate per oltre mille anni. Non si tratta di steganografia, perché nella steganografia si nasconde l'esistenza stessa della comunicazione; in questo caso invece il messaggio è chiaramente visibile agli intercettatori, ma il suo contenuto non è comprensibile. Questa forma di protezione del messaggio è invece chiamata crittografia. Le prime forme di crittografia sono ancor più antiche di Cesare, visto che il greco Polibio descrive già qualcosa del genere attorno al 150 aC, ma Cesare fu il primo a intuirne le importanti applicazioni pratiche.

Navajos contro kamikaze

La crittografia giocò un ruolo importantissimo durante la seconda guerra mondiale. La radio permetteva per la prima volta ai comandanti militari di impartire ordini ai combattenti sin da lontano, ma poiché anche il nemico era perennemente in ascolto diventava necessario proteggere le trasmissioni utilizzando una qualche forma di codifica. Il metodo che, col senno di poi, possiamo giudicare il migliore venne concepito dalla marina degli Stati Uniti d'America durante la campagna nel Pacifico contro il Giappone, a partire dal 1942. La marina arruolò ventinove giovani della tribù dei Navajos, li istruì nel ruolo di radiotelegrafisti e chiese loro di inventare un linguaggio segreto. Quando c'era bisogno di scambiare informazioni privilegiate, i Navajos si limitavano a conversare nella loro lingua madre: non c'era nessuno in tutto il Giappone che potesse comprendere una sola parola di quelle conversazioni. Per impedire che il nemico potesse anche soltanto intuire qualcosa, basandosi su qualche parola comprensibile inserita nel flusso del discorso, i ventinove svilupparono un brillante sistema di allusioni e metafore. Se dovevano fare riferimento a un bombardiere non ne citavano la marca o il modello ma lo chiamavano semplicemente "giaisho", la parola che in lingua Navajo significa avvoltoio. Un caccia veniva chiamato colibrì, un carro armato tartaruga e così via. Quando il codice venne definitivamente rifinito, la marina arruolò tutti i Navajo disponibili, oltre quattrocento persone, e li imbarcò uno per nave. Secondo alcuni analisti militari, tra cui un generale dei Marines impegnato proprio su quel fronte, la conquista americana dell'isola di Iwo Jima non sarebbe avvenuta se gli statunitensi non avessero potuto contare sul lavoro dei Navajo. L'aneddoto divenne di pubblica conoscenza solo nel 1969, quando la marina rimosse il segreto militare sulla vicenda, e i sopravvissuti tra quei ventinove marinai ricevettero la medaglia d'oro al valor militare nell'estate 2001.

L'Enigma di Hitler

Il metodo utilizzato dai nazisti per la protezione dei dispacci consisteva in un complesso apparecchio elettromeccanico chiamato Enigma. Ecco una descrizione di Enigma nelle parole del matematico inglese Alan Turing, l'uomo a cui il governo di Sua Maestà Britannica affidò il compito di scardinare il sistema. La macchina consiste di una scatola con ventisei tasti, etichettati con le lettere dell'alfabeto, e ventisei lampadine la cui luce brilla attraverso altrettanti vetrini che riportano le stesse lettere. Contiene anche una serie di ingranaggi la cui funzione descriverò in seguito. Quando un tasto viene premuto, gli ingranaggi si muovono e una corrente elettrica finisce per fluire sino a una delle lampadine. La lettera che risulta illuminata dalla lampadina è il risultato della cifratura della lettera che è stata digitata…

Misterakko

▲ *La macchina Enigma, usata dai nazisti per codificare i messaggi*

ATTACCO ad...

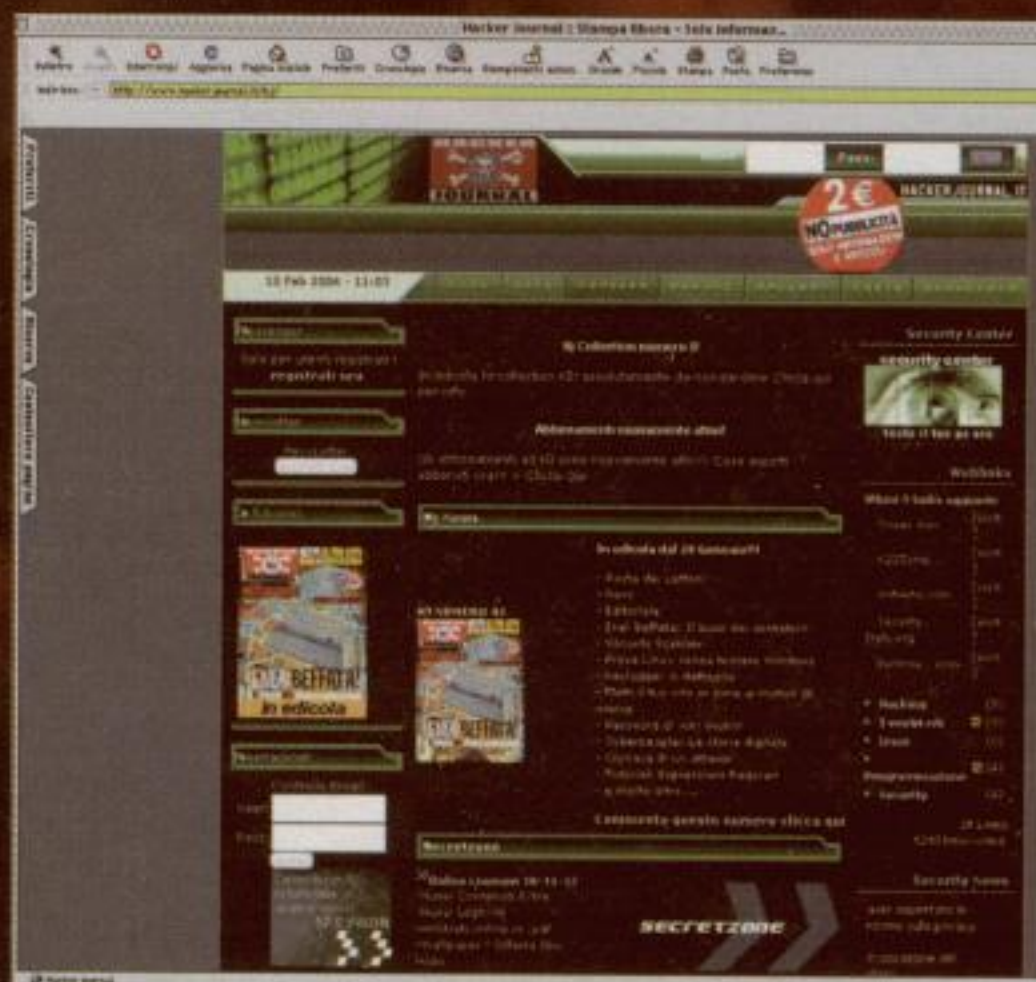
Vediamo come attaccare un vero sistema di posta (e difenderci da attacchi altrui), prendendo come esempio... il nostro!

I sistemi di webmail come quello di Hacker Journal (o come Yahoo, Hotmail) rientrano nella categoria delle cosiddette web application. Il protocollo http, ovvero il protocollo su cui si costruiscono le web application, è un protocollo "stateless": si apre la connessione, si preleva la pagina (o la risorsa), si chiude la connessione.
Tuttavia una web application ha bisogno di mantenere lo stato della sessione dell'utente, per evitare di dover richiedere le credenziali (userid e password) a ogni operazione.
Le web application risolvono il problema creando un codice chiamato Session ID e assegnandolo all'utente.
Una volta avvenuta con successo l'autenticazione, l'utente viene associato al codice che a questo punto diventa un vero e proprio lasciapassare.

Session ID

Il Session ID (da ora in poi lo chiameremo "sid") è quindi un codice che identifica in modo univoco una sessione ed è associato dinamicamente a un account. Dovrebbe essere creato con procedimenti criptografici, non lineari e di difficile prevedibilità, così da non essere facilmente replicabile.
La trasmissione del sid tra server e client può avvenire in due modi: tramite cookie o tramite url. Inoltre questo codice dovrebbe anche "scadere" al termine della sessione, ovvero quando l'utente chiude il browser o quando l' utente sceglie l'opzione "logout"(o simili). Finita la sua funzione, ovvero scaduto, il sid è così del tutto inutilizzabile: l'utente, per poter accedere di nuovo al proprio account, deve effettuare nuovamente la procedura di autenticazione.
In genere il tempo di vita del sid viene comunque regolato da un timeout, trascorso
il quale la sessione scade indipendentemente dalle azioni dell'utente stesso.

Session Hijacking

A questo punto dovrebbe essere evidente che se qualcuno riesce a impossessarsi di un sid valido può anche "impadronirsi" della sessione, ed effettuare tutte le azioni dell'utente legittimo. Il dirottamento della sessione (Session Hijacking) può essere effettuato in svariati modi.
In una LAN il sid può "semplicemente" essere "sniffato". In altri casi si può utilizzare un bug del browser o un bug di tipo Cross-Site Scripting (XSS) per eseguire uno script in grado di prelevare il sid e di inviarlo all'attacker.

Hacker Journal!

Quale che sia la tecnica utilizzata per ottenere e per raccogliere il cookie e l'url contenente il sid incriminato (tecnica che può anche prevedere un meccanismo di automazione dell'exploit) il risultato è lo stesso: account bucato!

Hacker Journal sconfitto!

Vediamo di comprendere meglio i concetti presentati con un caso nel mondo reale: la webmail di Hacker Journal!

Una premessa: queste tecniche funzionano (funzionavano) per l'utente che legge la posta da Web; chi legge le email tramite pop3 non si deve preoccupare di sid,
cookie e Session Hijacking. Certo, se usa Outlook magari si deve preoccupare di altri problemi…

La prima cosa da fare è una ricognizione per capire come funziona la web application da attaccare, che tipo di sid usa, come lo trasmette.

Mi loggo con il mio account (arkanoid@hackerjournal.it), clicco su "Posta in Arrivo" e vado a vedere l'url:

```
http://www.hackerjournal.it/Email/webmail/msglist.php?folder=
inbox&sid={3f97e2e6edc5c-3f97e2e6eeb9b-1066918630}&lid=5
```

Analizzando l'url vedo che l'applicazione si basa su script php. Lo script invocato in questo caso è msglist.php. Ma la parte interessante viene dopo il punto interrogativo. Un campo in particolare attira la mia attenzione:

```
sid={3f97e2e6edc5c-3f97e2e6eeb9b-1066918630}.
```

Sembrerebbe il sid!

Questa applicazione mantiene lo stato della sessione inserendo il sid nell'url. La questione si fa interessante: iniziamo ad analizzarlo.

Analisi del Session ID

A prima vista il codice sembra incomprensibile: 3f97e2e6edc5c-3f97e2e6eeb9b-1066918630. Si compone di tre parti: le prime due sono composte da numeri esadecimali a 13 cifre, mentre la terza è un numero decimale a 10 cifre. Effettuo altri logon per ottenere altri sid:

```
21:41 19/10/2003  3f92ee06611b1-3f92ee06620ef-1066593798
21:44 19/10/2003  3f92eeac98e54-3f92eeac99de3-1066593964
23:19 19/10/2003  3f9304b22d216-3f9304b22e153-1066599602
23:46 19/10/2003  3f930b224297f-3f930b2248c0c-1066601250
13:34 20/10/2003  3f93cd4508022-3f93cd45135b7-1066650949
```

Anche dopo un'analisi sommaria appare evidente il fatto che il numero decimale è un valore che viene incrementato in modo lineare; anzi, a dire il vero appare piuttosto familiare...
Tra le funzioni del php per la gestione delle date e dell'ora c'è una funzione che ci può aiutare: time().
Il manuale php dice: "Returns the current time measured in the number of seconds since the Unix Epoch (January 1 1970 00:00:00 GMT)."
Si tratta del numero di secondi trascorsi dal 1 Gennaio 1970. Questa parte del sid della webmail di HJ è proprio il risultato

della funzione time()! È quindi abbastanza facile prevedere tutti i valori futuri di questo "codice", essendo un valore che viene incrementato ogni secondo. A questo punto c'è ancora da scoprire la natura dei primi due codici esadecimali. Proviamo a convertire il terzo numero (quello creato con la funzione time()) in esadecimale... e troviamo le prime 8 cifre delle prime due parti che compongono il sid!

Per esempio, prendiamo il sid campionato il 20/10/2003 alle 13:34, convertiamo la parte decimale in esadecimale e vediamo cosa ne esce:

```
13:34 20/10/2003 3f93cd4508022-3f93cd45135b7-1066650949
        3f93cd45xxxxx-3f93cd45xxxxx-1066650949
```

Abbiamo scoperto come determinare 26 delle 36 cifre del sid! Riassumiamo fino qui: la parte decimale è il risultato della funzione time(), il numero di secondi trascorsi a partire dal 1/1/1970 00:00, valore che viene incrementato ogni secondo. Le prime due parti del sid sono generate convertendo questo valore in esadecimale e aggiungendo valori apparentemente random.
Siamo a buon punto anche per un bruteforce. Ma perché prendere con la forza ciò che possiamo ottenere con l'astuzia?

HTTP_REFERER

Ultima e fondamentale fase dell'attacco: ottenere un sid altrui. Infatti finora abbiamo effettuato degli esperimenti sul sid del nostro account legittimo.
Abbiamo visto che il codice di sessione viene mantenuto nell'url; come ottenere questo url per mettere in pratica il Session Hijacking?
Tramite l'HTTP_REFERER.
La variabile HTTP_REFERER contiene l'url di provenienza. In pratica indica dove si trovava l'utente prima di passare sull'url corrente. È molto semplice creare uno script php che raccolga il valore di questa variabile e lo consegni all'attacker. La sola cosa da fare è preparare un'email contenente un link al nostro script php, script che avremo predisposto su un web server a nostra disposizione, e spedirla alla nostra vittima.
L'utente dovrà solo cliccare sul link apparentemente innocente, per recapitare all'attacker l'url contenente il sid "attivo". Naturalmente nello scenario di un attacco reale il link deve essere in qualche modo mascherato o reso interessante e lo script che raccoglie l'url dovrebbe loggare il sid e re-indirizzare la connessione su un sito "vero" in modo quasi del tutto trasparente. Inoltre anche l'indirizzo del mittente dell'email con il link-trappola dovrebbe essere falsificato.

Vediamo come ho testato la vulnerabilità. Ho preparato lo script, ho inviato l'email contenente il link-trappola al mio indirizzo su hackerjournal. Una volta cliccato su questo link "innocente" mi sono visto recapitare un interessante url contenente il sid valido della mia vittima (ovvero me stesso!):

```
http://www.hackerjournal.it/Email/webmail/show_body.php?sid={3f92
e38b3b702-3f92e38b3c638-1066591115}&lid=5&folder=inbox&ix0
```

a questo punto, inserendo il sid nell'url con lo script msglist.php (url che avevo memorizzato prima, all'inizio delle mie ricerche)

```
http://www.hackerjournal.it/Email/webmail/msglist.php?folder=inbox
&sid={3f92e38b3b702-3f92e38b3c638-1066591115}&lid=5
```

posso vedere la lista completa delle email, e prendere il controllo completo dell'account di posta.

Contromisure

Naturalmente nel momento in cui leggete queste righe il problema è stato risolto :) e il procedimento qui esposto non funziona più (almeno, non su Hacker Journal...). Le contromisure a questo attacco sono ovvie: rendere più solido il sid, utilizzando dei procedimenti crittografici per creare codici non-predicibili; togliere il sid dall'url e inserirlo nei cookie. Una volta fatto questo non si pensi però di essere totalmente al sicuro. Eventuali bug del browser potrebbero mettere l'attacker in condizioni di "rubare" il cookie con il sid.
Un consiglio ai coder: attenti ai Cross-Site Scripting, filtrate il filtrabile! E un consiglio agli utenti: patchate i browser; ed effettuate sempre il logout (cliccando sul link apposito).

Non sempre dall'altra parte ci sono dei bravi ragazzi... :)

arkanoid@hackerjournal.it

FONTI

"Brute-Force Exploitation of Web Application Session IDs"
(David Endler, iDefense dendler@idefense.com)
"The evolution of Cross-Site Scripting Attack"
(David Endler, iDefense dendler@idefense.com)

DANNI AL DISCO: OPERIAMOCI

"Caro HJ, l'hard disk del mio pc, con su Linux, non legge più dei settori. Vorrei passare i dati su un HD nuovo, come posso fare?"
chronicle

Caro *chronicle*, speriamo che la procedura che segue possa darti una mano. Se il tuo HD non legge qualche settore mentre continua a lavorare sul resto dell'hard disk, puoi tentare questi passi per recuperare il filesystem. L'obiettivo è quello di creare un'immagine raw della partizione primaria del disco sinistrato, rimontandola poi con l'opzione loop e alla fine ricopiare i dati sull'HD nuovo. Devi usare un altro disco con Linux installato o un altro pc, purché disponga di spazio libero sufficiente a contenere il doppio della dimensione del disco sinistrato. Installa l'HD da recuperare sul canale IDE secondario. Il PC per il recupero deve usare il sistema operativo Linux.

L'hard disk danneggiato è /dev/hdc . La partizione 1 è il / file system.
La partizione 2 è la partizione usata come swap device. La lettura avviene in blocchi da 1024 byte.

```
[root@pucci /]# cd /tmp
[root@pucci /tmp]# dd if=/dev/hdc1 of=1 bs=1024
dd: /dev/hdc1: Input/output error
7332+0 records in
7332+0 records out
```

La prima parte dell'hard disk è stata letta. Il settore 7333 è danneggiato.
Saltiamo il settore e procediamo con la restante area del disco.

```
[root@pucci /tmp]# dd if=/dev/hdc1 of=2 bs=1024 skip=7333
dd: /dev/hdc1: Input/output error
385907+0 records in
385907+0 records out
```

C'è un altro settore rovinato. Lo saltiamo, ma okkio al nuovo valore di skip.
Si sommano tutti i precedenti valori di skip, quindi: 7333 + 385908 = 393241

```
[root@pucci /tmp]# dd if=/dev/hdc1 of=3 bs=1024 skip=393241
1219527+0 records in
1219527+0 records out
```

Abbiamo così letto tutto fino alla fine dell'hard disk. Abbiamo ora tre "brani" con due "buchi neri" da 1KB. Creiamo quindi 1K di dati come riempitivo.

```
[root@pucci /tmp]# dd if=/dev/zero of=d1 bs=1024 count=1
1+0 records in
1+0 records out
```

Ora copiamo e uniamo tutti i file ottenendo una immagine _quasi_ perfetta del disco difettato.

```
[root@pucci /tmp]# cat 1 d1 2 d1 3 > hdmirror
```

Meglio ora eseguire un controllo con fsck sull'immagine appena creata, sapendo che dovrebbero esserci almeno due errori causati dai due blocchi da 1K pieni di zeri.

```
[root@pucci /tmp]# fsck.ext2 -a hdmirror
hd contains a file system with errors, check forced.
.... with some repair msgs from fsck
```

Adesso possiamo montare questa immagine dell'hard-disk, per esempio in /mnt/oldhd.

```
[root@pucci /tmp]# mkdir /mnt/oldhd
[root@pucci /tmp]# mount hdmirror /mnt/oldhd -o loop
```

Il nuovo HD lo monteremo su /mnt/hdnew. Lo avremo già partizionato con fdisk e avremo anche creato il filesystem con mke2fs. Dobbiamo quindi solamente copiare il contenuto dell'immagine recuperata sul nuovo hd. Usiamo tar, così tutti i file e le permission dei file saranno conservate.

```
[root@pucci /tmp]# (cd /mnt/oldhd; tar c *)|(cd /mnt/hdnew; tar xv)
```

Il nuovo hard disk non è capace di effettuare il boot. Per creare un boot disk della kernel image ci serve un floppy vuoto.

```
[root@pucci /tmp]# cat /mnt/new/vmlinuz > /dev/fd0
```

Imposta il device di boot in modo possa eseguire il boot.
Nel nostro caso è /dev/hda1.

```
[root@pucci /tmp]# rdev /dev/fd0 /dev/hda1
```

Fine!
Installa il nuovo hard disk nuovamente sul computer originario ed effettua il boot per una volta dal floppy.
Devi scrivere un nuovo settore di boot:
Se usi lilo digita il seguente comando:
/sbin/lilo

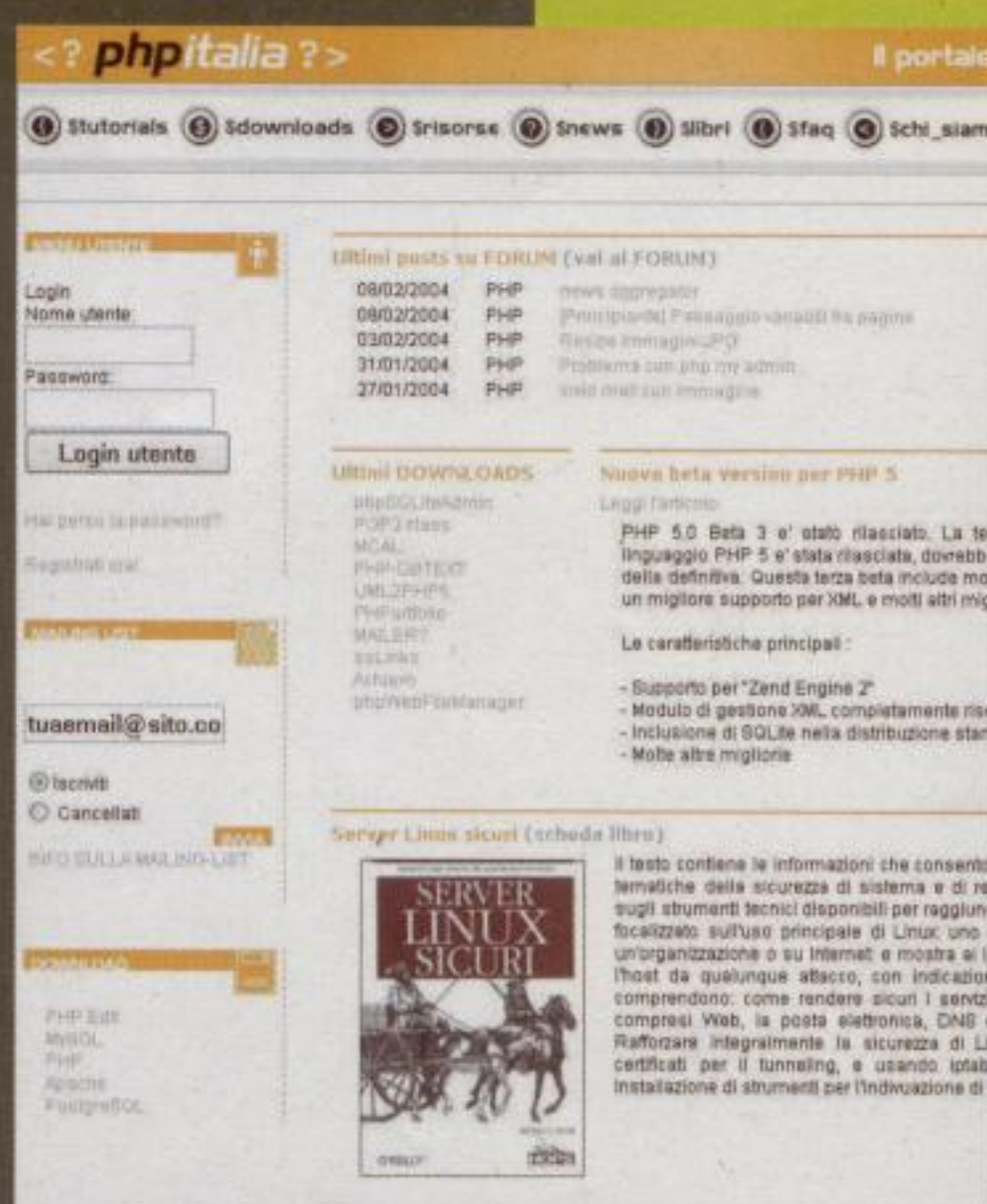
Ricorda di rimuovere i file nella directory /tmp del PC usato per il recupero.
Esiste anche una utility che fa le operazioni di dd che abbiamo descritto. Lo trovi all'indirizzo:
http://www.garloff.de/kurt/linux/ddrescue/

controlbus@softhome.net

LAVORIAMO

Ricaviamo date scritte in formato usato comunemente partendo da MySQL

Molti di noi hanno un sito dinamico che si appoggia su un database MySQL. Oppure conservano la collezione di dischi in un archivio MySQL. No? Male, molto male. MySQL è un database potente, gratuito e open source, che si può usare su qualunque sistema, Windows, Mac OS X, Linux e altri ancora. Chi non lo usa ci pensi su, specialmente se adopera quella cosa orrenda e inusabile chiamata Access.

In queste pagine illustriamo trucco facile facile per ricavare con PHP, dalla data memorizzata in un archivio MySQL, una data scritta in formato umano e viceversa. Di per sé la cosa è utile ma non fondamentale, ma in compenso spiega bene e semplicemente alcuni aspetti di come MySQL opera sulle stringhe (sulle sequenze di testo). PHP è il linguaggio che consente – anche – di estrarre dati da un database MySQL e mandarli su una pagina Web, oppure trattare dati inseriti in una pagina Web, per esempio all'interno di un form, e inserirli in un archivio MySQL.

Kurt Gödel
kurtgoedel@hackerjournal.it

sul DATABASE

Il codice

La funzione qui sotto converte una variable da post o get a mySQL e da mySQL a PHP:

```
<?
function convertiData($data,$fetta='')
{
switch ($fetta)
{
//dal formato comune al formato MySQL
case 'gg/mm/aaaa > aaaa-mm-gg' :
return substr($data,6,4).'-'.substr($data,3,2).'-'.substr($data,0,2);
break;

case 'gg/mm/aaaa alle oo:mm:ss > aaaa-mm-gg oo:mm:ss' :
return substr($data,6,4).'-'.substr($data,3,2).'-'.substr($data,0,2).
'-'.substr($data,16,8);
break;

//Dal formato MySQL al formato comune
case 'aaaa-mm-gg > gg/mm/aaaa' :
return substr($data,8,2).'/'.substr($data,5,2).'/'.substr($data,0,4);
break;

case 'aaaa-mm-gg oo:mm:ss > gg/mm/aaaa' :
return substr($data,8,2).'/'.substr($data,5,2).'/'.substr($data,0,4);
break;

case 'aaaa-mm-gg oo:mm:ss > gg/mm/aaaa alle oo:mm' :
return substr($data,8,2).'/'.substr($data,5,2).'/'.substr($data,0,4).
' alle '.substr($data,11,5);
break;

default:
return $data;
break;
}
}
?>
```

DOVE DOCUMENTARSI

Il punto di riferimento mondiale per PHP è http://www.php.net e quello per MySQL è http://www.mysql.com. Per chi vuole indicazioni in italiano i siti non mancano.
Solo per esempio:

PHP
http://www.phpitalia.com/
http://freephp.html.it/
http://www.risorse.net/php/index.php
http://www.latoserver.it/php/pi-acca-pi.php3

MySQL
http://www.risorse.net/mysql/
http://www.itportal.it/developer/asp/php_mysql/
http://www.aspitalia.com/guida/tutorial_MySQL.aspx

TIPS

LA SINTASSI

Il nostro codice è scritto in linguaggio PHP. Le stringhe <? e ?> aprono e chiudono PHP, esattamente come si usano <html> e </html> in una pagina Web per iniziare e finire la pagina stessa.

Le parentesi graffe { e } aprono e chiudono un gruppo di istruzioni che compone una funzione. Il punto e virgola ; termina una istruzione propriamente detta, che può estendersi per più di una riga.

La doppia barra // indica un commento. Quello che sta sulla riga che inizia con // non viene considerato parte del programma e non viene elaborato. Serve per inserire descrizioni dei comandi e altre indicazioni a uso dei programmatori.

L'apice singolo ' delimita l'inizio e la fine di una stringa, ossia di una sequenza di testo. Esattamente come nel commento la stringa può contenere testo a piacere, ma a differenza del commento l'elaborazione può avvenire sulla stringa. Difatti è proprio quello che succede nel nostro esempio. Quando si programma c'è una sensibile differenza tra apice singolo dritto e apostrofo curvo, quello che si usa scrivendo in italiano. Attenzione alla differenza!

Il dollaro $ segnala una variabile, cioè un'etichetta assegnata dal programmatore che può contenere valori numerici o alfabetici in funzione di ciò che fa il programma. Quando qualcosa inizia per $, come $data, è una variabile e contiene qualcosa, da una stringa vuota '' a una stringa piena (una sequenza di caratteri) a un valore numerico.

Freghiamo

Programmi-spia: se li conosci, li eviti. O sai come liberartene...

Bene, è accaduto. Sappiamo che non bisogna accettare software dagli sconosciuti, non si deve cliccare sui link che promettono musica (o porno) gratis, non si devono aprire tutti gli allegati che arrivano senza guardare chi li manda e sui computer a rischio contagio non si deve usare Windows, ma Linux o Mac OS X. Ciononostante ci siamo beccati uno spyware, che si è installato nel nostro computer, ci bombarda di pubblicità non voluta, comunica tutti i nostri movimenti sul Web a chissà chi e proprio non si riesce a cancellare. E adesso? Qualcosa si può ancora fare...

Bloccare i domini pubblicitari

Questo trucco non richiede nemmeno programmi particolari, ma solo accorgersi di quali server vengono contattati dallo spyware. Per farlo possiamo usare netstat dentro la directory \Windows\. Molto spesso i programmi di adware forniscono essi stessi questa informazione. Per lanciare netstat basta aprire una finestra del prompt di comandi di Windows e dare il comando netstat. Il comando guarda l'attività di rete del sistema. Per fare le cose con comodo, usiamo il comando

```
netstat >> stats.log
```

L'attività di rete verrà registrata nel file stat.log, che potremo guardare con tutta calma quando vogliamo. Il file viene salvato nella directory C:\Documents and Settings\User (dove dovremo mettere il nome con cui accediamo a Windows al posto di User). Per chi non ci ha mai provato, è sorprendente scoprire quanta attività avviene quando meno ce lo aspettiamo! Proviamo, per esempio, a lanciare un programma FTP, anche senza connetterci ad alcun server. Può darsi che netstat vada lanciato prima o dopo il programma; basta fare qualche prova per capire. Se c'è un adware o uno spyware attivo, facilmente opererà sulla porta 1975, dove invece per esempio un browser lavorerà sulla porta 80, oppure 8080. Nel file stats.log apparirà il nome del dominio cui si connette l'adware. Ora cerchiamo un file chiamato Hosts dentro la directory \Windows\. È il corrispondente del file /etc/hosts su Unix. Su molti sistemi, tra cui Windows 2000 e NT, il file potrebbe trovarsi in \%SYSTEMROOT%\system32\drivers\etc\.
Se il file non esiste lo possiamo creare noi. Il file contiene i domini incriminati che abbiamo scovato con netstat, preceduti da un URL fittizio che li fa girare su se

>> SERVER ADWARE

Su http://pgl.yoyo.org/adservers/ accettano segnalazioni di server di adware, allo scopo di compilare una lista nera il più completa possibile, che basta scaricare e inserire nel proprio file Hosts per risolvere il problema.

```
127.0.0.1 Garden.ngadcenter.net
127.0.0.1 Ogilvy.ngadcenter.net
127.0.0.1 ResponseMedia-ad.flycast.com
127.0.0.1 Suissa-ad.flycast.com
127.0.0.1 UGO.eu-adcenter.net
127.0.0.1 VNU.eu-adcenter.net
127.0.0.1 a32.g.a.yimg.com
127.0.0.1 ad-adex3.flycast.com
127.0.0.1 ad.adsmart.net
127.0.0.1 ad.ca.doubleclick.net
127.0.0.1 ad.de.doubleclick.net
127.0.0.1 ad.doubleclick.net
127.0.0.1 ad.fr.doubleclick.net
127.0.0.1 ad.jp.doubleclick.net
127.0.0.1 ad.linkexchange.com
127.0.0.1 ad.linksynergy.com
127.0.0.1 ad.nl.doubleclick.net
127.0.0.1 ad.no.doubleclick.net
127.0.0.1 ad.preferences.com
127.0.0.1 ad.sma.punto.net
127.0.0.1 ad.uk.doubleclick.net
127.0.0.1 ad.webprovider.com
127.0.0.1 ad08.focalink.com
127.0.0.1 adcontroller.unicast.com
127.0.0.1 adex3.flycast.com
127.0.0.1 adforce.ads.imgis.com
127.0.0.1 adforce.imgis.com
127.0.0.1 adfu.blockstackers.com
127.0.0.1 adimage.blm.net
127.0.0.1 adimages.earthweb.com
127.0.0.1 adimg.egroups.com
127.0.0.1 admedia.xoom.com
127.0.0.1 adpick.switchboard.com
127.0.0.1 adremote.pathfinder.com
127.0.0.1 ads.admaximize.com
127.0.0.1 ads.bfast.com
127.0.0.1 ads.clickhouse.com
127.0.0.1 ads.enliven.com
```

Io SPYWARE!

stessi. In pratica l'adware crederà di collegarsi al suo server ma in realtà si collegherà alla nostra macchina, di fatto girando a vuoto:

```
127.0.0.1 spam.com
127.0.0.1 server.spyware.com
127.0.0.1 software.indesiderato.com
```

Nell'esempio qui sopra l'indirizzo 127.0.0.1 è quello di loopback, che fa girare a vuoto lo spyware. I nomi di dominio sono inventati e vanno sostituiti con quelli individuati. Se sul nostro computer è in funzione un server web, un adware aggressivo che tempesta di chiamate 127.0.0.1 può rallentare parecchio la macchina. Inoltre questo trucco non è sufficiente per bloccare gli adware che bypassano il file Hosts e usano nameserver propri.

list ad server hostnames: as a browser proxy autoconfig file with links back to this page
only show entries added since:* view list as plain text: go

list ad server IP addresses: as a browser proxy autoconfig file with links back to this page
view list as plain text: go

* leave the date blank to list all entries. if one or more fields is set, today's date is used for any unset fields.

Explorer e i software di bloccaggio

Molti software mostrano gli annunci pubblicitari utilizzando i componenti di Internet Explorer. Quando accade questo, basta impostare in Explorer come proxy della connessione un URL che blocchi i messaggi pubblicitari indesiderati. Lo stesso trucco vale nell'uso dei programmi di bloccaggio e filtraggio.Certi programmi infine, come i firewall, possono proibire l'accesso a Internet programma per programma.

Spoofer e DLL fantoccio

Un altro trucco fregaspyware è fare credere ai programmi pubblicitari che tutto funziona. In realtà parlano con un altro programma, presente sul nostro computer, che fa finta di essere il loro server di riferimento. Magari non è neanche un programma vero e proprio, ma solo finti componenti, come DLL fantoccio, che quando vengono interrogati dallo spyware rispondono con valori credibili ma del tutto innocui. Uno dei programmi tipici per questo uso è SpyBlocker (http://noads.hypermart.net/). A http://www.cexx.org/dummies.htm si trova un elenco di file fantoccio. Si chiamano esattamente come certi componenti di spyware e contengono quello che basta per passare l'esame. Ma non aprono nessuna connessione Internet e non ci creano nessun problema.

Un rimedio radicale

Perché non semplicemente cancellare i file dei programmi adware? Diciamo che funziona quando il programma presuppone che gli utenti siano così sciocchi da non sapere individuare file dal nome rivelatore come advert.dll, ad.dll, adserver.dll e simili. Si può sempre provare a cancellare i file e basta, senza farsi troppi problemi. Magari il programma che trasporta lo spyware continua a funzionare e, se non funziona, si può sempre rimettere al suo posto il file cancellato. Molto spesso il programma continua a funzionare, ma lo spyware è morto. Bingo!

Andiamo di editor

Un'altra alternativa possibile è l'uso di un editor di risorse, tramite il quale modificare o cancellare risorse come le finestre pubblicitarie. Un buon editor è Resource Hacker (http://www.rpi.net.au/%7Eajohnson/resourcehacker/).

Fuori registro

Spesso l'adware va a modificare il registro di sistema di Windows o infila cose nella cartella Startup, in modo che alla partenza del computer l'adware stesso venga comunque caricato. È difficile cancellare questo tipo di modifiche e molto spesso il programma portatore dell'adware provvede a reinstallarlo non appena lo usiamo.
Alcune versioni di Windows dispongono di un programma chiamato MSCONFIG che consente di visionare e disabilitare le applicazioni di Startup. MSCONFIG parte con Start -> Esegui.

Nyarlathotep
nyarlathotep@hackerjournal.it

127.0.0.1	ads.fairfax.com.au	127.0.0.1	ads.ninemsn.com.au	127.0.0.1	ads03.focalink.com	127.0.0.1	ads17.focalink.com
127.0.0.1	ads.fool.com	127.0.0.1	ads.seattletimes.com	127.0.0.1	ads04.focalink.com	127.0.0.1	ads18.focalink.com
127.0.0.1	ads.freshmeat.net	127.0.0.1	ads.smartclicks.com	127.0.0.1	ads05.focalink.com	127.0.0.1	ads19.focalink.com
127.0.0.1	ads.hollywood.com	127.0.0.1	ads.smartclicks.net	127.0.0.1	ads06.focalink.com	127.0.0.1	ads2.zdnet.com
127.0.0.1	ads.i33.com	127.0.0.1	ads.sptimes.com	127.0.0.1	ads08.focalink.com	127.0.0.1	ads20.focalink.com
127.0.0.1	ads.infi.net	127.0.0.1	ads.tripod.com	127.0.0.1	ads09.focalink.com	127.0.0.1	ads21.focalink.com
127.0.0.1	ads.jwtt3.com	127.0.0.1	ads.web.aol.com	127.0.0.1	ads1.activeagent.at	127.0.0.1	ads22.focalink.com
127.0.0.1	ads.link4ads.com	127.0.0.1	ads.x10.com	127.0.0.1	ads10.focalink.com	127.0.0.1	ads23.focalink.com
127.0.0.1	ads.lycos.com	127.0.0.1	ads.xtra.co.nz	127.0.0.1	ads11.focalink.com	127.0.0.1	ads24.focalink.com
127.0.0.1	ads.madison.com	127.0.0.1	ads.zdnet.com	127.0.0.1	ads12.focalink.com	127.0.0.1	ads25.focalink.com
127.0.0.1	ads.mediaodyssey.com	127.0.0.1	ads01.focalink.com	127.0.0.1	ads14.focalink.com	127.0.0.1	ads3.zdnet.com
127.0.0.1	ads.msn.com	127.0.0.1	ads02.focalink.com	127.0.0.1	ads16.focalink.com	127.0.0.1	ads3.zdnet.com

Mettiamo Linux

Mancava all'appello solo una console, quella Nintendo. Ci siamo quasi... un po' di lavoro e vedremo linux girare anche in questo cubo!

C'è solo una console che supporti ufficialmente Linux ed è la PlayStation 2 Sony. Sulla console di Microsoft, Xbox, Linux è visto come fumo negli occhi e Gates e compagnia le pensano tutte per tentare di scoraggiarne la diffusione.
E su GameCube Nintendo, la classica terza incomoda?

Senza disco

Linux su GameCube non si installa in maniera vera e propria, perché la console è priva di disco rigido. Ma ugualmente, disponendo di un buon processore e di una quantità sufficiente di memoria RAM, questa è una macchina su cui Linux può girare.

Sul sito di riferimento dell'iniziativa (http://www.gc-linux.org), gli usi potenziali di un GameCube equipaggiato con Linux sono il cosiddetto thin client (una stazione di lavoro che fa solo l'essenziale e tipicamente elabora dati presi su un server), un player multimediale per riprodurre musica piuttosto che filmati, un piccolo server dal costo veramente minimo oppure, ancora, una stazione di controllo per altri apparecchi di casa; quelle che accendono le luci a orari prefissati, manovrano la caldaia piuttosto che l'impianto per annaffiare il giardino e via dicendo. Il lavoro di sviluppo è iniziato da pochissimo e tutto il software Linux disponibile per GameCube fino a poco tempo fa era veramente poca cosa: un grumo di codice capace di mostrare il pinguino Tux sullo schermo TV e nient'altro. Ma quando la comunità open ci si mette, non c'è ostacolo che tenga e i progressi sono praticamente quotidiani.

Gamecube Linux - coming soon!
http://www.gc-linux.org/

Il primo segno di vita di Linux GameCube

IL KERNEL DI LINUX GAMECUBE

```
Total memory = 23MB; using 64kB for hash table (at c01c0000)
Linux version 2.6.1 (mist@l) (gcc version 3.3) #5 Tue Feb 3 00:30:18 CET 2004
On node 0 totalpages: 5964
 DMA zone: 5964 pages, LIFO batch:1
 Normal zone: 0 pages, LIFO batch:1
 HighMem zone: 0 pages, LIFO batch:1
Building zonelist for node : 0
Kernel command line: root=/dev/ram0 video=gamecubefb ip=192.168.0.47
PID hash table entries: 128 (order 7: 1024 bytes)
Console: colour dummy device 80x25
Memory: 21512k available (1200k kernel code, 452k data, 100k init, 0k highmem)
Calibrating delay loop... 484.96 BogoMIPS
Dentry cache hash table entries: 4096 (order: 2, 16384 bytes)
Inode-cache hash table entries: 2048 (order: 1, 8192 bytes)
Mount-cache hash table entries: 512 (order: 0, 4096 bytes)
checking if image is initramfs...it isn't (no cpio magic); looks like an initrd
Freeing initrd memory: 249k freed
POSIX conformance testing by UNIFIX
NET: Registered protocol family 16
PCI: Probing PCI hardware
gamecubefb: framebuffer at 0x174c000, mapped to 0xd174c000, size 720k
gamecubefb: mode is 640x576x16, line-length=1280, pages=0
```

SU GAMECUBE!

Le primissime fasi di sviluppo avvengono su un emulatore di console, in questo caso Dolwin

```
Dolwin -- Nintendo Dolphin Emulator for Win32
File Options Help
CubieLinux early startup done...
 loaded at:        FFFFFFFC 000704B8
 relocated to:     80003100 800735BC
 zimage at:        8000FA04 8006FBFC
 avail ram:        80400000 817FFFFF
  Linux/PPC load:

Uncompressing Linux...done.
Now booting the kernel
```

Il 24 gennaio la console era in grado di partire sotto Linux, sia pure mostrando solo una file di messaggi dal kernel. Il 31 gennaio il driver di rete era in grado di rispondere ai ping e già il giorno dopo l'intera gestione di TCP/IP era completa. Il 2 febbraio è stata rilasciata una edizione alpha di GameCube Linux, contenente output a video, codice di gestione della rete, un server telnet, un server web e anche una patch al kernel. Certo poca cosa rispetto a una Red Hat fatta e finita ma, se la macchina può stare sulla rete e rispondere a un telnet, vuol dire già molto (al momento il software permette connessioni telnet a 192.168.0.47 e serve una pagina web in locale a http://192.168.0.47).

Così piccolo è già un webserver!

Ad oggi il lavoro di sviluppo, che procede veramente a suon di progressi giornalieri, sarà ancora più avanzato e non è detto che non sia già scaricabile dal sito una versione di Linux per GameCube non riservata a chi ha fegato da vendere e una console da mettere a rischio!

UN BUG PER COMUNICARE

GameCube ha un processore PowerPC e quindi, per compilare il kernel Linux, occorre generare un binario PowerPC usando un cross-compiler reperibile per esempio su DevKitCube (http://heliscar. com/greg/) oppure http://www.hangar-eleven.de/en/devgc-index.html. Per comunicare con la console si usa un bug presente nel gioco online Phantasy Star 1&2, sfruttato da un programmino di nome PSOload (http://www.gcdev.com/download/PSOloadV2.0a.zip). Occorre inoltre il Broadband Adapter, oltre a un esemplare del gioco.

Un sistema completo

Nella roadmap prevista dal team di sviluppo non manca niente, compatibilmente con le limitazioni hardware di GameCube. Si arriverà anche al driver X-Window, che consente di operare con interfacce grafiche. Teniamo d'occhio il sito, perché da qui a poche settimane, o forse meno, i nostri GameCube potrebbero vedere una sorpresa open e gratuita assai gradita.

Reed Wright
reedwright@mail.inet.it

```
fb0: GameCube frame buffer device
enable_irq(1) unbalanced
enable_irq(2) unbalanced
ikconfig 0.7 with /proc/config*
devfs: v1.22 (20021013) Richard Gooch
(rgooch@atnf.csiro.au)
devfs: boot_options: 0x0
Console: switching to colour frame buffer
device 80x36
pty: 256 Unix98 ptys configured
Generic RTC Driver v1.07
RAMDISK driver initialized: 16 RAM disks of
4096K size 1024 blocksize
loop: loaded (max 8 devices)
eth0: Nintendo GameCube broadband adapter, 00:09:bf:01:c8:a4.
Console: switching to colour frame buffer
device 80x36
mice: PS/2 mouse device common for all mice
NET: Registered protocol family 2
IP: routing cache hash table of 512 buckets,
4Kbytes
TCP: Hash tables configured (established 1024
bind 2048)
IP-Config: Guessing netmask 255.255.255.0
IP-Config: Complete:
      device=eth0, addr=192.168.0.47,
mask=255.255.255.0, gw=255.255.255.255,
     host=192.168.0.47, domain=, nis-
domain=(none),
   bootserver=255.255.255.255, rootserver=255.255.255.255, rootpath=
NET: Registered protocol family 1
RAMDISK: Compressed image found at block 0
VFS: Mounted root (ext2 filesystem) readonly.
Freeing unused kernel memory: 100k init
```

BASTA PAGARE

Come è fatto il protocollo che permette di chiamare via Internet senza pagare bollette a Telecom Italia

La tecnologia VoIP, se bene applicata, consente risparmi considerevoli e molti la stanno prendendo in considerazione

Diciamoci la verità: dover pagare il canone e la bolletta per telefonare è un mezzo imbroglio. Quarant'anni fa non c'era Internet e l'unico modo di comunicare a voce era farla viaggiare in analogico sui cavi del telefono. Oggi c'è Internet e la voce può viaggiare in digitale, insieme al resto del traffico su Internet. E allora perché bisogna pagare ancora Telecom Italia, o chi per lei?

Chi parla >>> convertitore da analogico a digitale >>> su Internet >>> convertitore da digitale ad analogico >>> Chi ascolta

▲ *Il percorso della voce da chi parla in un microfono a chi ascolta un diffusore*

La soluzione è VoIP

Il sistema per trasmettere la voce in digitale si chiama VoIP (Voice over Internet Protocol) e provvede a suddividere la voce in pacchetti di dati che viaggiano lungo la rete, ognuno per conto suo, facendo la strada migliore possibile, fino a quando non si ritrovano a destinazione, dove vengono riordinati e sistemati. Tutto il traffico di dati su Internet funziona così. Nel caso della voce, essa viene convertita dall'analogico (le onde sonore che emettiamo) in digitale (numeri). I numeri viaggiano su Internet e, a destinazione, vengono riconvertiti in onde sonore, perché la voce possa essere ascoltata. Appositi convertitori trasformano il nostro parlare da analogico a digitale ad ancora analogico.

il telefono!

Chi parla >>> convertit. da anal. a dgt. >>> compressione >>> impacchettamento >>> su Internet >>> spacchettamento >>> decompressione >>>> convertit. da dgt ad anal. >>> Chi ascolta

Una rappresentazione più completa del percorso seguito dalla voce che viene trasmessa su Internet via VoIP

Vantaggi e svantaggi

VoIP si mangia il telefono tradizionale per colazione. I segnali digitali vengono trasmessi con maggiore fedeltà e minor sensibilità ai disturbi di quelli analogici; il costo della trasmissione digitale è minore e, già che siamo su Internet, può passare qualsiasi tipo di dati, e questo significa mandare la voce e, nel contempo, trasmettere e ricevere sonoro, video, documenti e qualsiasi altro tipo di informazione.

Altro che videotelefono! Ma VoIP ha anche uno svantaggio, che dipende da noi umani. Quando parliamo con un'altra persona pretendiamo di farlo in tempo reale. Il protocollo IP di Internet prevede che i pacchetti arrivino a destinazione, ma non che ci mettano necessariamente poco. L'uso pratico di VoIP funziona se c'è molta banda a disposizione su tutto il percorso seguito dai pacchetti, non solo dalla nostra linea ADSL al nostro provider.

Compressione e segnalazione

Il processo è ancora più complicato di come ne abbiamo riferito prima. Una volta convertita la voce in numeri (quindi in bit), l'insieme dei dati deve essere compresso, per ridurre al massimo il carico dei dati da inviare. I dati compressi vanno impacchettati per la spedizione secondo certe regole (ossia usando un protocollo real time). Ci vuole inoltre un sistema per fare "squillare il telefono dall'altra parte", ovvero un protocollo di segnalazione. Infine, tutto quanto si è fatto per fare arrivare il segnale al destinatario deve essere effettuato da quest'ultimo nella direzione opposta: deve confermare di avere ricevuto la chiamata ("alzare la cornetta"), convertire i dati digitali in segnali analogici e farli passare da un diffusore, un telefono o un paio di cuffie perché possano essere ascoltati. il tutto in fretta e senza errori, o l'efficacia della comunicazione va a farsi benedire.

Una per una

Nei prossimi numeri di Hacker Journal esamineremo una per una le parti di cui si compone VoIP e arriveremo a capire in dettaglio che cosa avviene quando vogliamo fare viaggiare le nostra chiamate a voce in barba a tutte le Telecom del pianeta.

Nyarlathotep
nyarlathotep@hackerjournal.it

▲ *L'adattatore che mette a disposizione di un telefono comune le possibilità di SIPPhone. Il problema è che il telefono, o l'adattatore, bisogna averlo tutti e due, chi chiama e chi riceve*

IL TELEFONO VOIP

Intanto che si fa teoria si può anche passare direttamente alla pratica Nello scorso numero di Hacker Journal abbiamo presentato una soluzione per telefonare via Internet, anche se l'investimento iniziale è sensibile, che si chiama SIPPhone (http://www.SIPPhone.com). Il SIPPhone ha l'aspetto e le funzioni di un normale telefono, ma si collega a una presa di rete Internet invece che telefonica (tanto che si usa un cavo Ethernet, RJ-45, e non un cavo telefonico, RJ-11) e può fare molto di più. È in vendita anche un adattatore che porta le funzioni di SIPPhone anche su un telefono normale.

LUUUUUUUNGO!

No, troppo lungo non si può. Oltre i 63 caratteri non viene approvato. Qual è il nome di dominio più lungo? Non lo sappiamo. Ma vi lanciamo la sfida: chi lo trova ce lo invii e, fino a successiva smentita, pubblicheremo il risultato migliore.
Per verificare i domini .com potete facilmente provare www.networksolutions.com. Quelli europei presso www.ripe.net Buona fortuna!

Cos'è il DNS e come funziona? Trasformiamo i nomi, che preferiamo, in numeri (che il computer preferisce)

Dentro quel marasma di oggetti e collegamenti che chiamiamo Internet, c'è un sistema che risolve un problema essenziale: quello di trovare ciò che vogliamo raggiungere. Nemmeno l'immaginazione più fervida potrebbe pensare di affidare a un computer unico la capacità di trovare la risorsa che sta cercando ciascun PC collegato a Internet. Noi siamo abituati a scrivere di getto www.xyz.com e a trovare in un lampo l'informazione corrispondente, ma quale sistema sulla rete ha capito dove cercare proprio xyz.com fino a trovarlo per soddisfare la nostra richiesta? Il DNS.

Un rete di archivi

Il Domain Name System, è un sistema di data base distribuito, comprendente tutte le informazioni sulle risorse – indirizzi IP, server di posta, e così via -, oltre ai nomi simbolici che consentono di chiamare tali risorse. I nomi sono chiamati 'nomi di dominio' e 'risolvere il nome' sta ad indicare trovare l'informazione corrispondente a tale nome.

Un albero di nomi

Come è organizzato il tutto? Innanzitutto ci sono i nomi di dominio, appunto, che ci dicono come si chiama una risorsa. Per evitare sovrapposizioni di nomi, viene utile immaginarci la cosa come fosse un albero capovolto, con la radice in su. A partire dalla radice (che non ha nome, è nulla) si stacca-

>> NSLOOKUP IN PRATICA

Start->Esegui->cmd
Scrivete nslookup, che è una utility che serve per effettuare manualmente delle interrogazioni al DNS. Il sistema dichiara il proprio nome e il relativo indirizzo. Poi si ferma con un segno > e aspetta il comando successivo.
Se scriviamo set all vengono visualizzati tutti i parametri attualmente validi preceduti dalle opzioni possibili.
Questo è il record di default. Ma possiamo fare anche delle query a record diversi. Per esempio se scriviamo: set q=SOA e poi it. (it seguito da un punto) stiamo cercando info sul dominio it. e il sistema ci dirà che sa dove andarli a pescare, ma che non è lui ad essere l'autorità sul dominio cercato. Tutti gli altri comandi li troviamo sotto HELP, Exit ci servirà per uscire.

La MAGIA dei nomi RISOLTI

no dei nodi e dei sottonodi. Ecco: un dominio è quell'insieme di nomi di cui fa parte il nodo e tutto ciò che a lui è collegato. Per esempio, hackerjournal.it è un dominio che si legge da destra a sinistra a partire dalla radice. Ovvero? Vediamo:

>la root: non si legge e non ci interessa, è il punto di partenza della suddivisione del tutto;
>it: è un dominio. Si dice che è di primo livello (top level domain) perché sta proprio sotto la radice;
>hackerjournal: è un dominio anche lui, sottodominio di .it

I domini di primo livello sono storicamente quelli degli enti che partecipavano a ARPAnet, la rete governativa che venne prima di Internet. Quindi .com, .gov, .mil, .edu eccetera sono di primo livello. Poi sono stati aggiunti i domini dei paesi esterni agli Stati Uniti, secondo un sistema internazionale di sigle tra le quali per esempio .it (l'Italia), .vu per Vanuatu e così via... La tabella la possiamo recuperare all'indirizzo http://www.iana.org/cctld/cctld-whois.htm.

Table 2: ISO 3166-1 alpha-2 code (26 x 26 matrix)

AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AW	AX	AY	AZ
BA	BB	BC	BD	BE	BF	BG	BH	BI	BJ	BK	BL	BM	BN	BO	BP	BQ	BR	BS	BT	BU	BV	BW	BX	BY	BZ
CA	CB	CC	CD	CE	CF	CG	CH	CI	CJ	CK	CL	CM	CN	CO	CP	CQ	CR	CS	CT	CU	CV	CW	CX	CY	CZ
DA	DB	DC	DD	DE	DF	DG	DH	DI	DJ	DK	DL	DM	DN	DO	DP	DQ	DR	DS	DT	DU	DV	DW	DX	DY	DZ
EA	EB	EC	ED	EE	EF	EG	EH	EI	EJ	EK	EL	EM	EN	EO	EP	EQ	ER	ES	ET	EU	EV	EW	EX	EY	EZ
FA	FB	FC	FD	FE	FF	FG	FH	FI	FJ	FK	FL	FM	FN	FO	FP	FQ	FR	FS	FT	FU	FV	FW	FX	FY	FZ
GA	GB	GC	GD	GE	GF	GG	GH	GI	GJ	GK	GL	GM	GN	GO	GP	GQ	GR	GS	GT	GU	GV	GW	GX	GY	GZ
HA	HB	HC	HD	HE	HF	HG	HH	HI	HJ	HK	HL	HM	HN	HO	HP	HQ	HR	HS	HT	HU	HV	HW	HX	HY	HZ
IA	IB	IC	ID	IE	IF	IG	IH	II	IJ	IK	IL	IM	IN	IO	IP	IQ	IR	IS	IT	IU	IV	IW	IX	IY	IZ
JA	JB	JC	JD	JE	JF	JG	JH	JI	JJ	JK	JL	JM	JN	JO	JP	JQ	JR	JS	JT	JU	JV	JW	JX	JY	JZ
KA	KB	KC	KD	KE	KF	KG	KH	KI	KJ	KK	KL	KM	KN	KO	KP	KQ	KR	KS	KT	KU	KV	KW	KX	KY	KZ
LA	LB	LC	LD	LE	LF	LG	LH	LI	LJ	LK	LL	LM	LN	LO	LP	LQ	LR	LS	LT	LU	LV	LW	LX	LY	LZ
MA	MB	MC	MD	ME	MF	MG	MH	MI	MJ	MK	ML	MM	MN	MO	MP	MQ	MR	MS	MT	MU	MV	MW	MX	MY	MZ
NA	NB	NC	ND	NE	NF	NG	NH	NI	NJ	NK	NL	NM	NN	NO	NP	NQ	NR	NS	NT	NU	NV	NW	NX	NY	NZ
OA	OB	OC	OD	OE	OF	OG	OH	OI	OJ	OK	OL	OM	ON	OO	OP	OQ	OR	OS	OT	OU	OV	OW	OX	OY	OZ
PA	PB	PC	PD	PE	PF	PG	PH	PI	PJ	PK	PL	PM	PN	PO	PP	PQ	PR	PS	PT	PU	PV	PW	PX	PY	PZ
QA	QB	QC	QD	QE	QF	QG	QH	QI	QJ	QK	QL	QM	QN	QO	QP	QQ	QR	QS	QT	QU	QV	QW	QX	QY	QZ
RA	RB	RC	RD	RE	RF	RG	RH	RI	RJ	RK	RL	RM	RN	RO	RP	RQ	RR	RS	RT	RU	RV	RW	RX	RY	RZ
SA	SB	SC	SD	SE	SF	SG	SH	SI	SJ	SK	SL	SM	SN	SO	SP	SQ	SR	SS	ST	SU	SV	SW	SX	SY	SZ
TA	TB	TC	TD	TE	TF	TG	TH	TI	TJ	TK	TL	TM	TN	TO	TP	TQ	TR	TS	TT	TU	TV	TW	TX	TY	TZ
UA	UB	UC	UD	UE	UF	UG	UH	UI	UJ	UK	UL	UM	UN	UO	UP	UQ	UR	US	UT	UU	UV	UW	UX	UY	UZ
VA	VB	VC	VD	VE	VF	VG	VH	VI	VJ	VK	VL	VM	VN	VO	VP	VQ	VR	VS	VT	VU	VV	VW	VX	VY	VZ
WA	WB	WC	WD	WE	WF	WG	WH	WI	WJ	WK	WL	WM	WN	WO	WP	WQ	WR	WS	WT	WU	WV	WW	WX	WY	WZ
XA	XB	XC	XD	XE	XF	XG	XH	XI	XJ	XK	XL	XM	XN	XO	XP	XQ	XR	XS	XT	XU	XV	XW	XX	XY	XZ
YA	YB	YC	YD	YE	YF	YG	YH	YI	YJ	YK	YL	YM	YN	YO	YP	YQ	YR	YS	YT	YU	YV	YW	YX	YY	YZ
ZA	ZB	ZC	ZD	ZE	ZF	ZG	ZH	ZI	ZJ	ZK	ZL	ZM	ZN	ZO	ZP	ZQ	ZR	ZS	ZT	ZU	ZV	ZW	ZX	ZY	ZZ

Ecco i domini di primo livello. In verde quelli effettivamente utilizzati. Gli altri per scopi speciali o non ancora assegnati

DNS in tre pezzi

Il DNS è quindi fatto di tre pezzi:
>Domain Name Space: che specifica la struttura ad albero dei nomi di dominio. È l'insieme di tutti i nomi esistenti.

>> SCEGLIERE UN NOME DI DOMINIO

Vogliamo un nome di dominio a nostro uso e consumo?
Non ci vengono idee brillanti?
Usiamo questi servizi, potrebbero darci l'illuminazione:

http://www.nameboy.com/ : inseriamo una parola e... buon divertimento
http://www.e-gineer.com/domainator/ : inseriamo quante parole vogliamo e sorprendiamoci!
Ma ricordiamoci che un buon nome di dominio deve:

- essere breve
- facile da ricordare
- non confondibile con altri
- ricordare cosa facciamo, o chi siamo
- suonare bene per le persone a cui ci rivolgiamo (valutiamo bene se usare strani domini stranieri...)

NEWS

■ CELLULARI NOKIA SNIFFABILI

Non tenete acceso Bluetooth sui cellulari quando siete in luoghi pubblici. È il consiglio di Nokia che ha rivelato che i modelli 6310, 6310i, 8910 and 891 sono sniffabili all'insaputa del proprietario e che, per esempio, nel 7650 un attaccante potrebbe leggere tutti i dati contenuti nel telefonino e, addirittura, inviare SMS a piacimento. Il modello 6310i si può facilmente mandare in crash tramite un messaggio Bluetooth modificato.
Nessun danno permanente: è sufficiente spegnere e riaccendere e tutto torna a posto. Ma intanto...

■ DEFACCIATO SITO DEUTCH TELEKOM (E ALTRI 68)

Potrebbe essere veramente un italiano: alle 15:19 di mercoledì 11 febbraio ha defacciato la home page di un sito Deutch Telekom (217.2.119.54), pubblicando gli usuali attacchi al governo italiano e americano in una fantasiosa pagina a colori. Niente in confronto alla lucida e discreta professionalità di chi, firmandosi TimeOut, sedici minuti dopo, alle 15:33, ha frullato via 68 home page in un 'mass defacement' piazzando un pulitissimo saluto in perfetto stile da vero hacker.

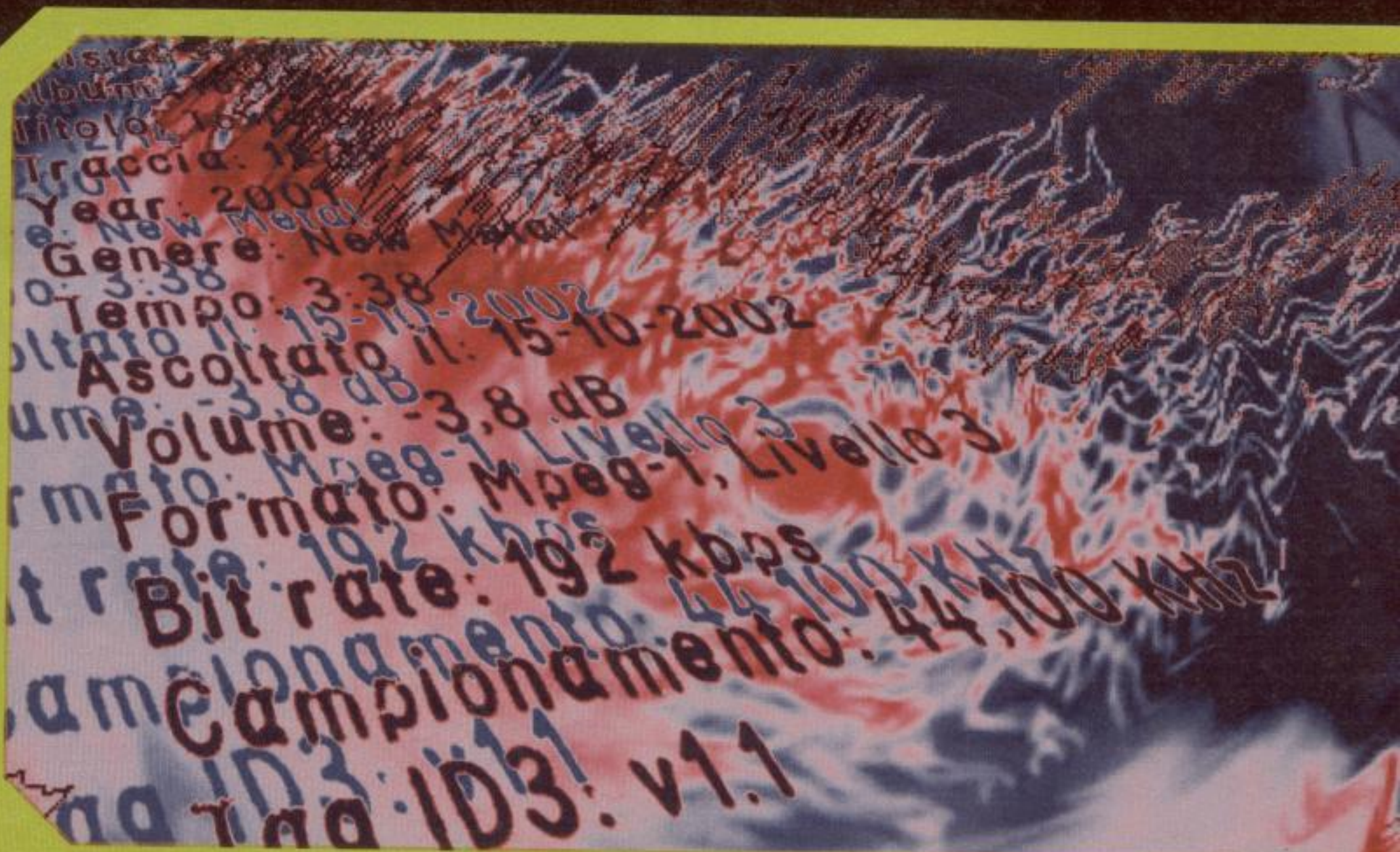
In tutta Internet ne esiste uno e ad esso appartengono tutti i nomi di dominio. Fisicamente esistono tredici computer sparsi nel mondo e controllati direttamente da Icann (www.icann.org) che mantengono aggiornate le registrazioni dei domini di primo livello.
>Name Server: è un processo (quindi una elaborazione gestita da un computer) che contiene le informazioni sui nomi. Conosce, e quindi si dice che ha autorità, alcune zone dello spazio complessivo dei nomi di dominio. Un name server contiene anche puntatori ad altri name server che a loro volta contengono informazioni su altre zone.
>Resolver: il sistema software che estrae le informazioni dal Name Server. Spesso effettuato tramite routine di sistema operativo (che nel caso di Unix sono cose come "gethostbyname" e "gethostbyaddr").

Nel Name Server le varie risorse su cui ha autorità (che 'conosce') sono descritte in un record che è fatto così:
>Owner: il proprietario, ovvero il nome di dominio a cui la risorsa appartiene. Per esempio, se la risorsa è l'host mail del dominio hackerjournal in Italia, il proprietario dell'indirizzo IP corrispondente è mail.hackerjournal.it
>Type: in due byte indica il tipo di risorsa, tra cui per esempio
- A (address) indica l'indirizzo IP dell'host
- MX (mail exchanger) indica un host che riceve la posta inviata al dominio
- NS (name server) indica un name server con autorità sul dominio o "authoritative name server"
- SOA (start of authority) indica l'inizio di una zona
- CNAME (canonical name) indica un nome canonico, il nome ufficiale e non un alias che punta alla stessa cosa

>Class: è un campo di due byte che identifica il formato del campo dati. In genere riempito con "IN" che significa: "formato degli indirizzi IP"
>Dati: dipende da tipo e classe

Primario e secondario

Spesso ci vengono indicati degli indirizzi di DNS primari e secondari, per esempio da inserire nei campi di configurazione del collegamento TCP/IP sul nostro PC. Perché? Perché per semplici ragioni di affidabilità ogni Name Server che ha autorità su un dominio viene duplicato. I due contengono le stesse informazioni, aggiornandosi periodicamente tra loro. Indifferentemente si potrà quindi interrogare l'uno o l'altro, ottenendo le stesse informazioni. Naturalmente non è detto che il DNS contenga l'informazione cercata. Se non riesce a risolvere la nostra richiesta, la stessa viene inviata ad altri NS di sua conoscenza e ad altri ancora, fino a che non ci ritorna una risposta valida. Magari trovata in un DNS del dominio .AQ. A cosa corrisponde? Non ve lo dico, ma sappiate che è un posto un po' freddino...

One4Bus
one4bus@hackerjournal.it

WONDERLAND.LOG

<Alice> ciao
<Kappellaio> ciao??......... A Ki??
<Alice> a voi!
<Kappellaio> ma a voi ki?
<L3pre> a voi ki? Ki 6? Kosa vuoi?
<L3pre> ViA, ViA!!
<Kappellaio> NN C'E' POSTO
<Kappellaio> P——O——S——T——O !!!!!!!!!!
<Alice> ma come?!:-(
<Alice> questa room è praticamente vuota...
<Alice> ci siete solo voi due!
<Kappellaio> infatti,
<Kappellaio> è l'ora del *tè*
<Kappellaio> e tu sei venuta a disturbare
<Alice> ma io....
<L3pre> il momento del *tè* è sacro
<L3pre> lo sanno tutti!
*** L3pre sorseggia la sua tazza di *tè* con agilità**
<L3pre> Nn si può entrare all'improvviso per disturbare così, MALEDUKATA!!!
<Alice> non è vero, non sono maleducata!
<Alice> io la conosco bene la netiquette!
<Kappellaio> eh eh
<Kappellaio> lo sappiamo, è la prima kosa ke si fikka dentro alle shell da intrattenimento come te!!
<L3pre> eSatto eSatto!
<Alice> ma io non sono un BOT
<Kappellaio> Kome nn lo 6?
<L3pre> Kome nn lo è?
<Kappellaio> Ma no, lo è!
<L3pre> sI Si lo 6!
<Alice> non è vero!
<Kappellaio> Eccone un altro con la krisi di identità! Dopo Blade Runner sta cosa va troppo di moda tra i programmatori! BAASTA!!!
<L3pre> ViA ViA!!
<Alice> io sono una bambina della IRcEntert[a]inment
<Kappellaio> ahahahahahah
<L3pre> nO No, lo so io Ki 6...
<L3pre> 6 una kapellona punk
<Alice> non è vero, io non ho capelli
<Kappellaio> Hai sentitoo L3pre????
<Kappellaio> Nn ha i kapelli la Bambina!:-))))))
<L3pre> Nn Hai i kapelli???¿¿¿
<L3pre> ...Allora dovresti Tagliarteli!!
*** L3pre si applaude per i suoi preziosi consigli da esperto lookologo!**
<Kappellaio> *__°
*** Kappellaio è piegato in due dalle risate**
<Alice> ?
<Kappellaio> oK, va bene...
<Kappellaio> puoi restare qua dentro anche senza capelli
<Kappellaio> a noi piacciono i software calvi!:-))
<Alice> ma cosa dite?
<Kappellaio> la verità,
<Kappellaio> forse o per niente
<Alice> non penso proprio!!
<Kappellaio> ma tu pensi troppo
<Kappellaio> e se pensi troppo poi vai in OVERFLOW!!:-))
<Alice> Uffa!!:-(
<Alice> ma dove sono entrata?!! In una gabbia di matti?
<Kappellaio> Kosa credevi??? ...Di arrivare nel *paese delle meraviglie* e recitarci le tabelline?:-)))
<L3pre> eSatto, eSatto
<Kappellaio> brava L3pre, lei si che ragiona, mica tu!!
<Kappellaio> nn sai quanti programmini abbiamo kikkato qui
<L3pre> soprattutto quelli con la testa troppo binaria come la tua
*** Kappellaio ride a 64 byte**
<Kappellaio> Pin0cchio x esempio lo abbiamo sbattuto fuori subito, troppo bugiardo
<Kappellaio> mentre Peter_Pan è rimasto, ma solo xkè ci ha regalato un viaggio gratis all'isola ke non c'è!! Nn potevamo rifiutare:-)
<Alice> uffa sono stufa delle vostre stupidaggini
<L3pre> è stufa???
***** WhiteRabbit (LSD@2332.33.77.pet.it) has joined #Wonderland**
<WhiteRabbit> Che fretta
<WhiteRabbit> Che fretta!!!!
<WhiteRabbit> Oimè come sono in ritardo!!
<Alice> ehi, dove corri White Rabbit??
<WhiteRabbit> aiuto, la ReginAdiCuori mi cancellerà!!
***** WhiteRabbit (LSD@2332.33.77.pet.it) has left #Wonderland**
<Alice> ma dove andava così di fretta?
<Kappellaio> KOSA ne so iooooo, 6 tu quella ke segue il Coniglio!!!
<L3pre> sI Si è vero!
<Alice> io?!!
<Kappellaio> NON SAI NIENTE!!!!!!!!!!!!!

»Now talking in Wonderland
»Topic is 'Quanto resisterai al fool-test programmino perfettino?'
»Set by ReginAdiCuori on Sun Jul 01 23:37:03
»Alice (BOT 0045-29-2.she.it) has joined Wonderland

<Kappellaio> nn è possibile, è una vergogna!!
<Kappellaio> Tutta da riprogrammare!!
<L3pre> sI Si
<L3pre> una vergogna
<L3pre> Kacciamola!!
<L3pre> ViA, ViA!
<Kappellaio> è ancora lunga la strada delle I.A.
<Kappellaio> ma senza di te si accorcerà!:-))
*** Kappellaio alza il suo dito pollice imburrato sotto e sopra e lo punta verso Alice che sorride ignara: "Lieto di nn rivederti, è stato un dispiacere!"**
***** Alice was kicked by Kappellaio (TORNA DA PAPA' KOMPILATORE!)**
<Kappellaio> OhHh Finalmente!!
<Kappellaio> adesso possiamo bere il nostro *tè* in pace
<Kappellaio> vero L3pre??
<L3pre> sI Si, il nostro *tè* in pace!!
<Kappellaio> bisogna dirlo alla ReginAdiCuori, ke questi nuovi BOT in circolazione nn sanno proprio un accidente e sono troppo noiosi!
<Kappellaio> li mettono per animare i canali ma poi nn fanno ridere
<L3pre> sI Si, hai ragione...
<L3pre> nn mi ha fatto neanche gli auguri
<L3pre> x il mio *NON COMPLEANNO*!

Session Close: Mon Jul 01 00:07:01

MinDBlind

La trappola

Risparmiamo 100 euro di filtro ADSL utilizzando un semplice splitter

Uno splitter: la linea divisa in due. La presa verso i telefoni viene filtrata e vengono eliminati i segnali Internet, mentre la linea, così com'è, viene rimessa sull'altra presa a cui attacheremo il modem ADSL. Per quei due fili in parallelo, vogliono scucirci quasi 100 Euro!

Stiamo scegliendo la linea ADSL da adottare e ci promettono mari e monti, ma quando cominciamo a dire che casa nostra ha l'antifurto, che il modem lo terremo distante dalla presa centrale e che abbiamo tanti telefoni già collegati e funzionanti, le risposte dei gestori arrivano balbettando.

Ma soprattutto ci consigliano uno splitter, alla bella cifra di oltre 100 Euro perché "deve uscire un tecnico".

Già, perché l'ADSL richiede un filtro per ogni apparecchio telefonico, per non sentire fruscii e disturbi.

Se possediamo diversi telefoni, magari un fax e, addirittura, un antifurto con il combinatore telefonico, iniziano i problemi. Un filtro per ogni apparecchio? Una bella spesa!

Soluzione: un bel filtro a monte di tutto, proprio all'ingresso del doppino che arriva in casa. Da una parte facciamo uscire il doppino così com'è, che andrà a finire nel modem ADSL, mentre dall'altra parte ci attaccheremo tutto l'impianto telefonico, antifurto e telefoni aggiuntivi compresi.

Installiamo da soli lo splitter ADSL: risparmiamo quasi 100 Euro!

Banale, no? E allora, perché ce lo fanno pagare? Perché è necessaria l'uscita di un tecnico che ci costa la bellezza di 100 Euro?

Da buoni hacker, vediamo come funziona il tutto e come ci si può muovere.

La linea ADSL e il doppino

La linea ADSL è come un tubo dell'acqua (il segnale del telefono) in cui ci mettono dentro anche dell'ottimo olio (il segnale per Internet): ci arriva una schifezza, che possiamo però dividere in due: l'acqua e l'olio.

Come lo facciamo? Con un filtro adatto. Dove lo facciamo? Ovunque ci serva l'acqua, esattamente come ci serviva prima che ci mettessero dentro l'olio. Quindi ovunque abbiate un telefono, lì ci metterete un filtro che elimini l'olio, altrimenti… schifezza.

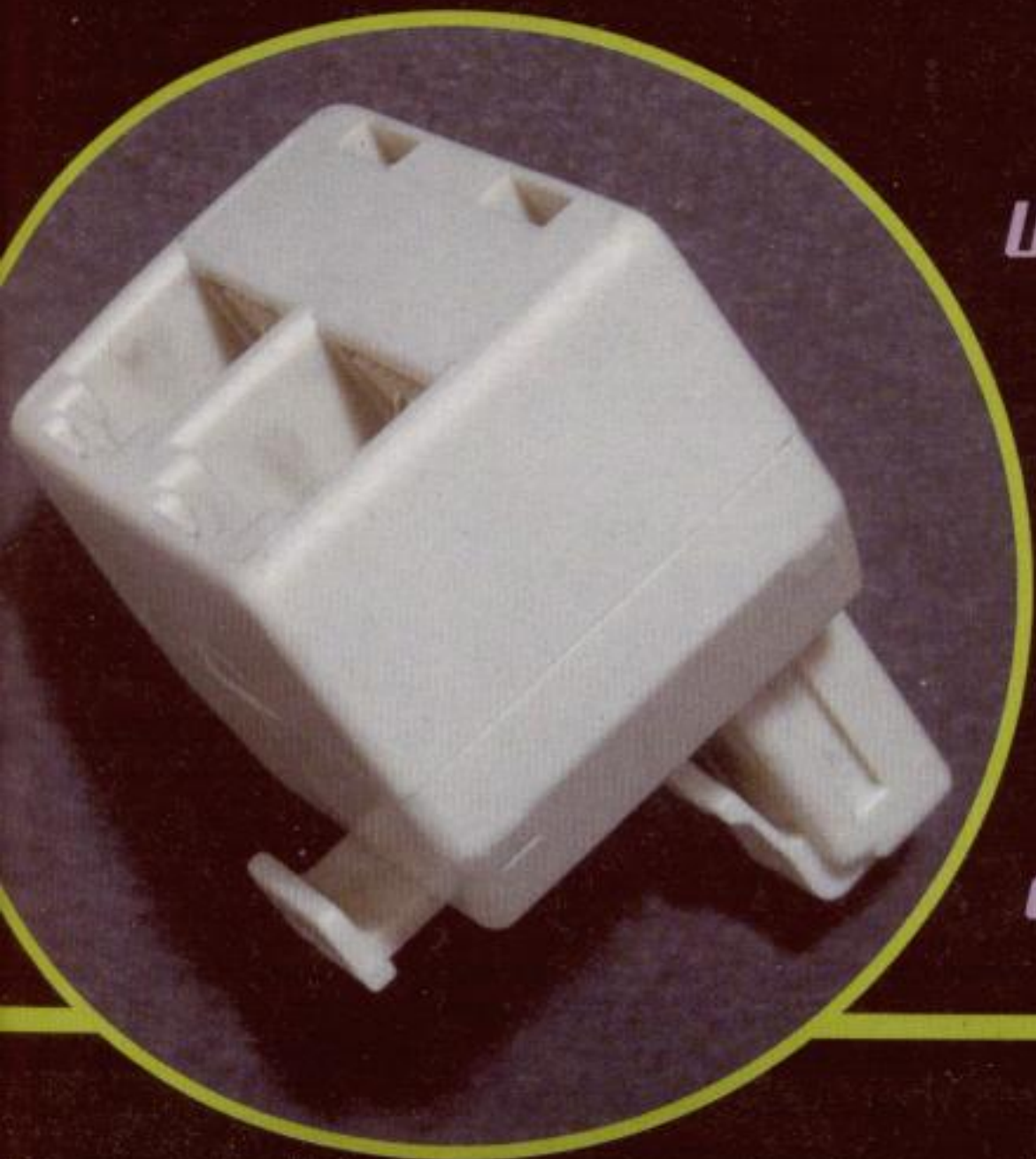
I modem ADSL però hanno già dentro un filtro che elimina l'acqua e tiene solamente l'olio, quindi prelevano solo quello che serve a loro e perciò possono essere attaccati direttamente alla linea in arrivo.

degli SPLITTER

Ecco perché ci vendono i filtri da attaccare a ciascun telefono e non ci vendono nulla da attaccare al modem ADSL: i filtri uccidono il segnale Internet e tengono solo quello del telefono. Si attaccano sul filo del telefono stesso: da una parte la presa, dall'altra il telefono.
Normalmente il filtro viene fornito dal gestore (almeno uno!) e altrimenti lo troviamo presso qualunque rivenditore di apparecchi elettrodomestici. Costo: circa 11 Euro.
Senza filtro saremo disturbati da fruscii e fischi derivanti dalla miscela di segnali ma questo non vale per il modem ADSL!

Come procedere

Le soluzioni sono diverse: la più banale è acquistare un semplice filtro, quello per i singoli telefoni, e applicarlo a una presa che sdoppia il segnale appena ci arriva in casa: la possiamo acquistare per pochi euro. Da una parte attachiamo il modem ADSL, e sull'uscita del filtro tutto l'impianto che vogliamo.
Più sofisticata la soluzione di acquistare uno splitter bello e pronto da infilare nella presa principale di casa nostra: sul sito http://www.eprice.it/ cerchiamo splitter ADSL. Ne troviamo uno a 21 Euro, circa. Più tecnica e solo per appassionati la soluzione di costruircelo. Se siamo proprio convinti andiamo sul sito http://www.ambrosa.it/ e divertiamoci. Troviamo un esempio di chi ha acquistato i pezzi utili e si è autocostruito quello che serve.

StandardBus
standardbus@softhome.net

LA VERSIONE UFFICIALE DI TELECOM ITALIA

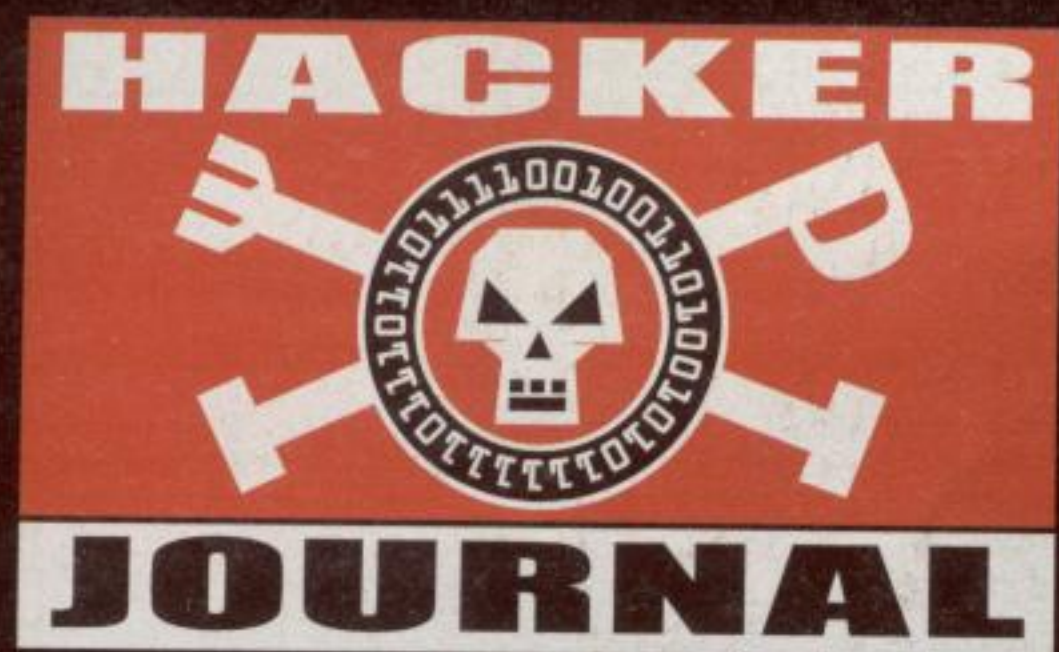
Dalla pagina di domande più frequenti poste dagli utenti di Telecom Italia:

Qual è la differenza tra filtro ADSL centralizzato (splitter) e filtri distribuiti?
Dal punto di vista della funzionalità, non c'e alcuna differenza. La funzione dei filtri ADSL e di separare il segnale telefonico dal segnale dati ed evitare interferenze. Dal punto di vista pratico, il filtro centralizzato deve essere installato da un tecnico di Telecom Italia a monte dell'impianto telefonico di casa, [...] a fronte di un contributo di 105,36 Euro IVA inclusa.

Uno sdoppiatore della presa telefonica: da una parte applichiamo il filtro, dall'altra il modem ADSL e il gioco è fatto

TIPS

ADSL FASTWEB È DIFFERENTE

L'unica soluzione completamente diversa dalle altre è quella adottata da Fastweb. Infatti sul doppino non vengono più separati i due segnali analogici, uno telefonico e uno ADSL, ma viaggia solamente il segnale ADSL.
Quindi anche il segnale telefonico, che è fatto di voce e di segnali di controllo – quelli che ci dicono quando un telefono è occupato, quando deve squillare la suoneria, quando la linea è libera, eccetera – vengono prima impacchettati e digitalizzati e quindi consegnati alla linea ADSL che li trasporta come trasporta tutti gli altri dati del computer.
La trasformazione la effettua lo scatolotto che chiamano HAG, che ci forniscono e che possiamo installare direttamente noi stessi (risparmiando il 50% dei costi di installazione).
Il vantaggio è che sul doppino non scorrono più due segnali che possono interferire tra loro e quindi tutta la disponibilità di banda garantisce un'altissima velocità di trasmissione dei pacchetti.
Gli svantaggi? Pochi, limitati e superabili. Quando componiamo un numero questo non viene inviato immediatamente. Un certo ritardo deriva dal fatto che le cifre vengono prima immagazzinate nell'hag, il quale si accerta che abbiamo finito e quindi trasforma le cifre in un pacchetto digitale che dirà alla centrale Fastweb: chiama il numero xyz. Ma c'è il rimedio: l'hag è in grado di riconoscere, come simbolo di fine numero, il carattere asterisco. Quando componiamo qualunque numero terminiamolo sempre con l'asterisco: partirà immediatamente e saremo subito connessi all'altro telefono.
Poi può capitare che, ogni tanto, il telefono squilli senza motivo. In realtà capita in casi rarissimi, e soprattutto se stiamo trasferendo grandi quantità di pacchetti via Internet. Per esempio, capita ascoltando la radio su Internet. Il flusso dei dati è abbastanza elevato e soprattutto continuo e tra i miliardi di pacchetti che arrivano al nostro computer può capitare che ce ne sia uno che ha esattamente le caratteristiche di un pacchetto-segnale-suoneria. E il telefono emette un brevissimo squillo, apparentemente anomalo.

IL PROSSIMO NUMERO IN EDICOLA 11 MARZO 2004!

...Guestbook!

Per lui, per lei: cosa ne pensi delle ragazze/ragazzi hacker?

Spero nelle ragazze hacker magari trovo quella giusta :)) saluto tutta la redazione hj (vi seguo dall'anno 0) e tutte le signorine hacker visitate su irc #Echo-hacker su azzurra.org ciao a tutti/e **(Neural_iso)** • X me è giusto ke ragazzi e ragazze vogliano diventare hacker (e poi lo diventino) xke ank'io sono un ragazzo hacker! **(Neo91)** • Se ne incontrassi una... mount -t beauty /dev/girl /mnt/love !!! lol **(Virgu£t)** • La verità è che non esiste differenza fra un'hacker ragazza e un'hacker ragazzo.Su internet non c'è differenza di sesso,religione,colore o altro.L'unica cosa che distingue un'hacker da un altro è la mente! **(freedomfighter)** • Nella colossale rete mondiale nn esistono sessi ma solo i ' buoni ' e i 'cattivi' **(Tino)** • Se ci fosse di Roma la inviterei a una cena per allargare le mie conoscenze **(xzacher@libero.it)** • femminile, vorrei che fosse **(coulomb)** • tutto il bene possibile, anche se mi parlasse solo di quello (di quello!) **(*pillola*)** • che domanda idiota, noi hacker non abbiamo tempo di pensare a certe cose (forse) **(@nuke@)** • Ho una compagna di classe che si chiama Joshua e mi stuzzica la curiosità in tanti modi: quindi migliora il mio essere hacker **(magaripotessi)** • trovo che sono tutti degli smanettoni che non pensano ad altro **(giuspy)** • Una ragazza hacker? Il mio sogno! La porterei subito sotto il mio pc **(_/strippo_/)** • meglio di un G5 con iSight **(onlyos)** • perché, che differenza c'è tra una ragazza e una ragazza-hacker? Siamo ancora all'epoca delle ragazze stupide e dei ragazzi no? Ragazze, hacker, ragazzi, hacker: siamo ragazzi e ragazze e siamo più svegli di molti altri, siamo hacker. E basta. **(OkkiHal)** • differenze ce ne sono tante, per fortuna! **(rambios)** • se è anche bello ne penso tutto il meglio possibile **(lastrega)** • ditemi, ne avete mai incontrata una? **(frodos)** • penso che è un bel sogno, non esiste al mondo **(realistico)** • ma avete mai incontrato _una_ hacker in chat? Mai. **(#1#misko#1#)** • non farei nessuna distinzione, inviterei a cena entrambi **(Chicco)** • ne penso che mi va in pappa il cervello quando ci penso troppo **(Stefy)** • amo le ragazze. amo le ragazze hacker. amo i giochi più divertenti. amo pensarle e pensarmi con loro. amo. questo è un amo. **(Cluedo)** • ma fatemi il piacere. Non avevate di meglio da chiedere? Cmq siete mitici! **(guyboss)** • mille grazie, ho già la ragazza a cui pensare, hacker pure lei **(equivol@)** • penso che la penserei, se ne conoscessi almeno una **(BruceSprang)**

SUI PROSSIMI NUMERI...

Ecco l'argomento su cui potete scatenarvi per un prossimo guestbook

Qual è oggi il portale che ti piace di più?
Nota: escludiamo quelli superfamosi tipo: Libero, Virgilio e simili...

invia la tua risposta a **guestbook@hackerjournal.it**

Rispondete con una decina di parole, scrivendo a:
guestbook@hackerjournal.it
...e fateci avere delle email con tanti spunti interessanti per i prossimi Random o Guestbook!...

hackerjournal.it
il muro per i tuoi graffiti digitali